



# **AVG Internet Security – Senza limiti**

Manuale per l'utente

**Revisione documento AVG.07 (25/11/2016)**

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



## Sommario

<b>1. Introduzione</b>	<b>4</b>
1.1 Requisiti hardware	4
1.2 Requisiti software	5
<b>2. AVG Zen</b>	<b>6</b>
2.1 Processo di installazione di Zen	7
2.2 Interfaccia utente di Zen	8
2.2.1 Riquadri delle categorie	8
2.2.2 Area dei dispositivi	8
2.2.3 Pulsante Messaggi	8
2.2.4 Pulsante dello stato	8
2.2.5 Pulsante Aggiorna / Rinnova	8
2.2.6 Pulsante Aggiorna	8
2.2.7 Pulsante delle impostazioni	8
2.2.8 Icona dell'area di notifica	8
2.3 Procedure dettagliate	20
2.3.1 Come accettare gli inviti	20
2.3.2 Come aggiungere dispositivi alla rete	20
2.3.3 Come modificare il nome o il tipo di dispositivo	20
2.3.4 Come connettersi a una rete Zen esistente	20
2.3.5 Come creare una nuova rete Zen	20
2.3.6 Come installare i prodotti AVG	20
2.3.7 Come abbandonare una rete	20
2.3.8 Come rimuovere i dispositivi dalla rete	20
2.3.9 Come visualizzare e/o gestire i prodotti AVG	20
2.4 Domande frequenti e assistenza	34
<b>3. AVG Internet Security</b>	<b>35</b>
3.1 Processo di installazione di AVG	36
3.1.1 Finestra introduttiva	36
3.1.2 Installazione di AVG	36
3.2 Dopo l'installazione	37
3.2.1 Aggiornamento del database dei virus	37
3.2.2 Registrazione del prodotto	37
3.2.3 Accesso all'interfaccia utente	37
3.2.4 Scansione dell'intero computer	37
3.2.5 Controllo Eicar	37
3.2.6 Configurazione predefinita di AVG	37
3.3 Interfaccia utente di AVG	39
3.3.1 Menu di spostamento superiore	39
3.3.2 Informazioni sullo stato di protezione	39
3.3.3 Panoramica dei componenti	39





3.3.4	<i>Collegamenti rapidi Scansione / Aggiornamento</i>	39
3.3.5	<i>AVG Advisor</i>	39
3.3.6	<i>AVG Accelerator</i>	39
3.4	<b>Componenti di AVG</b>	46
3.4.1	<i>Protezione del computer</i>	46
3.4.2	<i>Protezione esplorazione Web</i>	46
3.4.3	<i>Analisi del software</i>	46
3.4.4	<i>Protezione email</i>	46
3.4.5	<i>Firewall</i>	46
3.4.6	<i>PC Analyzer</i>	46
3.5	<b>Impostazioni avanzate di AVG</b>	58
3.5.1	<i>Aspetto</i>	58
3.5.2	<i>Suoni</i>	58
3.5.3	<i>Disattivazione temporanea della protezione di AVG</i>	58
3.5.4	<i>Protezione del computer</i>	58
3.5.5	<i>Scansione Email</i>	58
3.5.6	<i>Protezione esplorazione Web</i>	58
3.5.7	<i>Analisi del software</i>	58
3.5.8	<i>Scansioni</i>	58
3.5.9	<i>Pianificazioni</i>	58
3.5.10	<i>Aggiornamento</i>	58
3.5.11	<i>Eccezioni</i>	58
3.5.12	<i>Quarantena virus</i>	58
3.5.13	<i>Autoprotezione di AVG</i>	58
3.5.14	<i>Preferenze privacy</i>	58
3.5.15	<i>Ignora lo stato di errore</i>	58
3.5.16	<i>Avviso - Reti note</i>	58
3.6	<b>Impostazioni di Firewall</b>	109
3.6.1	<i>Generale</i>	109
3.6.2	<i>Applicazioni</i>	109
3.6.3	<i>Condivisione file e stampanti</i>	109
3.6.4	<i>Impostazioni avanzate</i>	109
3.6.5	<i>Reti definite</i>	109
3.6.6	<i>Servizi di sistema</i>	109
3.6.7	<i>Log</i>	109
3.7	<b>Scansione AVG</b>	119
3.7.1	<i>Scansioni predefinite</i>	119
3.7.2	<i>Scansione in Esplora risorse</i>	119
3.7.3	<i>Scansione dalla riga di comando</i>	119
3.7.4	<i>Pianificazione di scansioni</i>	119
3.7.5	<i>Risultati scansione</i>	119
3.7.6	<i>Dettagli di Risultati scansione</i>	119
3.8	<b>AVG File Shredder</b>	143



3.9 Quarantena virus	144
3.10 Cronologia	145
3.10.1 Risultati scansione	145
3.10.2 Risultati di Resident Shield	145
3.10.3 Risultati di Identity Protection	145
3.10.4 Risultati di Protezione email	145
3.10.5 Risultati di Online Shield	145
3.10.6 Cronologia eventi	145
3.10.7 Log Firewall	145
3.11 Aggiornamenti di AVG	155
3.12 Domande frequenti e assistenza tecnica	155





# 1. Introduzione

Grazie per avere acquistato il pacchetto **AVG Internet Security – Senza limiti!** Questo pacchetto consente di utilizzare tutte le funzionalità di **AVG Internet Security**, ora ottimizzate con **AVG Zen**.

## **AVG Zen**

Questo prezioso strumento di gestione assicura la protezione di tutta la famiglia. Tutti i dispositivi sono raccolti in un'unica posizione, per tenere traccia dello stato relativo a protezione, prestazioni e privacy in modo semplice e rapido per ciascun dispositivo. Grazie a **AVG Zen** non è più necessario controllare ogni singolo dispositivo. È perfino possibile eseguire le attività di scansione e manutenzione e correggere in remoto i problemi di sicurezza più urgenti. **AVG Zen** è integrato nel pacchetto, quindi funziona automaticamente fin dall'inizio.

[Per ulteriori informazioni su AVG Zen, fare clic qui](#)

## **AVG Internet Security**

Grazie ai diversi livelli di protezione per tutte le attività online offerti da questa pluripremiata applicazione, il furto d'identità, i virus o l'accesso ai siti pericolosi non sono più un problema. Con le funzionalità AVG Protective Cloud Technology e AVG Community Protection Network incluse nel pacchetto, le informazioni sulle minacce più recenti vengono raccolte e condivise con la community per assicurare una protezione ottimale. È possibile effettuare acquisti e usufruire dei servizi di banking online in modo sicuro, utilizzare i social network o esplorare ed eseguire ricerche in tutta sicurezza con la protezione in tempo reale.

[Per ulteriori informazioni su AVG Internet Security, fare clic qui](#)

## **1.1. Requisiti hardware**

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

- CPU Intel Pentium da 1,5 GHz o superiore
- 512 MB (Windows XP) / 1024 MB (Windows Vista, 7 e 8) di memoria RAM
- 1,3 GB di spazio libero sul disco rigido *(per l'installazione)*

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

- CPU Intel Pentium da 1,8 GHz o superiore
- 512 MB (Windows XP) / 1024 MB (Windows Vista, 7 e 8) di memoria RAM
- 1,6 GB di spazio libero sul disco rigido *(per l'installazione)*



## 1.2. Requisiti software

**AVG Internet Security** consente di proteggere le workstation che eseguono i seguenti sistemi operativi:

- Windows XP Home Edition SP3
- Windows XP Professional SP3
- Windows Vista (x86 e x64, tutte le edizioni)
- Windows 7 (x86 e x64, tutte le edizioni)
- Windows 8 (x32 e x64)
- Windows 10 (x32 e x64)

*(ed eventuali Service Pack successivi per sistemi operativi specifici)*





## 2. AVG Zen

**Questa sezione del manuale per l'utente fornisce la documentazione completa relativa a AVG Zen. Tenere presente che questo manuale descrive solamente la versione per PC del prodotto.**

AVG, uno dei principali sviluppatori di software per la protezione a livello mondiale, ha elaborato una nuova soluzione per soddisfare le esigenze dei propri clienti in materia di sicurezza. Il nuovo prodotto AVG Zen consente di connettere in modo efficace i dati, i dispositivi (dai computer desktop ai dispositivi mobili) e le persone che li utilizzano in un unico pacchetto progettato per semplificare la vita digitale degli utenti. Grazie a una singola applicazione, AVG Zen consente agli utenti di visualizzare rapidamente le impostazioni per la protezione e la privacy di tutti i propri dispositivi da un'unica posizione.

L'idea alla base dello sviluppo di AVG Zen è restituire all'utente di tutti questi dispositivi il controllo dei propri dati e della propria sicurezza, perché per AVG controllo è sinonimo di scelta. Lo scopo di AVG, infatti, non è cercare di convincere gli utenti che la condivisione o il tracciamento siano attività di per sé negative, quanto piuttosto fornire loro tutte le informazioni utili per controllare gli elementi condivisi e l'eventuale tracciamento delle attività, in modo da poter prendere decisioni consapevoli. Per AVG gli utenti devono poter vivere la propria vita in completa libertà, senza il timore di veder violata la propria privacy nella vita familiare di tutti i giorni o durante la ricerca di un nuovo lavoro.

Un altro vantaggio di AVG Zen è che offre ai clienti un'esperienza utente uniforme in tutti i dispositivi, in modo che anche i meno esperti possano imparare rapidamente a gestire e proteggere più dispositivi con semplicità. In un mondo sempre più complesso, almeno una cosa diventa più facile. Per concludere, è fondamentale ricordare che AVG Zen è progettato appositamente per assicurare agli utenti la tranquillità più completa, in qualsiasi momento. Man mano che Internet diventa il centro di questo mondo connesso, AVG Zen è la soluzione ideale per tenere tutto sotto controllo.

In questa parte della documentazione vengono descritte alcune funzionalità specifiche di AVG Zen. Qualora siano necessarie informazioni su altri prodotti AVG, consultare l'altra parte della documentazione o i manuali per l'utente distinti. È possibile scaricare questi manuali dal [sito Web di AVG](#).



## 2.1. Processo di installazione di Zen

Utilizzare la seguente [pagina Web](#) per acquistare e scaricare il pacchetto **AVG Internet Security – Senza limiti**. È possibile completare la procedura di installazione di AVG Internet Security in pochi semplici passaggi (fare clic qui per ulteriori informazioni). Nel corso della procedura viene installato anche AVG Zen. Subito dopo aver completato l'installazione, viene visualizzata l'interfaccia utente di [Zen](#). È possibile scegliere di creare una nuova rete Zen o di entrare a far parte di una rete esistente. Questa operazione tuttavia è facoltativa: è possibile saltare questo passaggio e utilizzare l'opzione di connessione alla rete Zen in un secondo momento.


**È possibile consultare i seguenti argomenti correlati:**

- [Presentazione delle tre modalità utente di AVG Zen](#)
- [Come accettare gli inviti](#)
- [Come connettersi a una rete Zen esistente](#)
- [Come creare una nuova rete Zen](#)



## 2.2. Interfaccia utente di Zen



Questa è la finestra di dialogo principale dell'interfaccia utente di AVG Zen. In tutte le altre finestre di dialogo è disponibile il pulsante  nell'angolo superiore sinistro, che permette di tornare alla schermata principale (se è presente una serie di finestre consecutive questo pulsante permette di tornare solamente alla finestra precedente).

Questa finestra di dialogo presenta diverse sezioni:

- [Riquadri delle categorie](#)
- [Area dei dispositivi](#)
- [Pulsante Messaggi](#)
- [Pulsante dello stato](#)
- [Pulsante Aggiorna / Rinnova](#)
- [Pulsante Aggiorna](#)
- [Pulsante delle impostazioni](#)
- [Icona dell'area di notifica](#)



## 2.2.1. Riquadri delle categorie



I riquadri delle categorie consentono di installare i prodotti software AVG, visualizzarne lo stato e anche aprirne l'interfaccia utente. L'[amministratore](#) della rete Zen può anche utilizzarli per visualizzare e gestire i prodotti AVG installati sui dispositivi remoti. Utilizzare l'[area dei dispositivi](#) per scorrere tutti i dispositivi remoti disponibili nella rete Zen.

In ogni riquadro è presente un cerchio, il cui colore dipende dallo stato dei prodotti in relazione alla relativa categoria (in una situazione ottimale, i cerchi dovrebbero essere sempre verdi). Per alcune categorie, è possibile visualizzare solo un semicerchio, che significa che si dispone già di un prodotto di questa categoria, ma è possibile installarne un altro.

Anche se i riquadri visualizzati sono gli stessi per qualsiasi dispositivo, il contenuto potrebbe variare a seconda del tipo di dispositivo monitorato ([PC](#), [Android](#) o [Mac](#)).

### 2.2.1.1. PC

#### INTERNET SECURITY / ANTIVIRUS FREE

**AVG Internet Security:** grazie ai diversi livelli di protezione per tutte le attività online offerti da questo software, il furto d'identità, i virus o l'accesso ai siti pericolosi non sono più un problema. Con le funzionalità Tecnologia di protezione cloud AVG e Rete di protezione della community AVG incluse nel prodotto, le informazioni sulle minacce più recenti vengono raccolte e condivise con la community per fornire una protezione ottimale. È possibile effettuare acquisti e usufruire dei servizi di banking online in modo sicuro, utilizzare i social network o esplorare ed eseguire ricerche in tutta sicurezza con la protezione in tempo reale.

**AVG AntiVirus Free:** in alternativa, è possibile utilizzare gratuitamente la protezione di base del computer. AVG AntiVirus Free offre affidabili capacità di protezione da virus, spyware e malware, collegamenti Web dannosi e furto di identità. Non include tuttavia funzionalità aggiuntive quali Firewall, Anti-Spam, Archivio dati protetto, gli aggiornamenti prioritari e l'assistenza premium.

#### Panoramica degli stati

- Se né AVG Internet Security né AVG AntiVirus FREE sono installati, questo riquadro non è attivo (visualizzato in grigio) e il testo sottostante indica "Protezione non attiva". È tuttavia sufficiente fare clic sul riquadro per [installare questa applicazione AVG](#).
- Se è presente un numero elevato di problemi da correggere (ad esempio quando l'intera protezione è disattivata), il cerchio all'interno del riquadro diventa rosso e il testo sottostante indica "Protezione non attiva". Se sono presenti solo pochi problemi di minore entità, il cerchio all'interno del riquadro viene visualizzato in verde, ma il testo sottostante indicherà "Protezione parziale". In entrambi i casi, verrà visualizzato un numero all'interno di un cerchio colorato (nell'angolo superiore destro del riquadro) che indica il numero di problemi che è possibile correggere. Utilizzare il [pulsante Messaggi](#) per visualizzare un elenco dei problemi ed eventualmente risolverli.





- Se non sono presenti problemi, il cerchio all'interno del riquadro viene visualizzato in verde e il testo sottostante indica "Protezione completa".

Cosa succede quando si seleziona questo riquadro:

- Se nel computer non è ancora stata installata una soluzione di protezione, viene visualizzata una finestra di dialogo che permette di installare il prodotto. [Ulteriori informazioni sull'installazione dei prodotti AVG.](#)
- Quando si visualizzano i dispositivi con AVG Internet Security o AVG AntiVirus FREE installato, si apre l'interfaccia utente del prodotto.
- Quando si visualizza (come [amministratore](#)) un dispositivo remoto con AVG Internet Security o AVG AntiVirus installato, si apre una finestra di dialogo con una breve panoramica dello stato dell'applicazione in tale dispositivo. Questa finestra di dialogo consente di eseguire diverse operazioni in remoto, ad esempio una scansione (con il pulsante **Esegui scansione**) o un aggiornamento (con il pulsante **Aggiorna**). Per accedere ad altre operazioni in remoto (ad esempio l'attivazione di componenti di protezione precedentemente disattivati), fare clic sul pulsante **Mostra dettagli** che consente di aprire la [finestra di dialogo dei messaggi](#) per i dispositivi selezionati. [Ulteriori informazioni sulla visualizzazione e la gestione dei dispositivi remoti.](#)

## PC TUNEUP

**AVG PC TuneUp** è l'applicazione che consente di ripristinare le prestazioni ottimali di sistema operativo, giochi e programmi. AVG PC TuneUp consente inoltre di eseguire importanti attività di manutenzione, come la pulizia del disco rigido e del registro di sistema in modo automatico o manuale. Questa applicazione consente di individuare eventuali problemi presenti nel sistema e propone rapide soluzioni. È inoltre possibile utilizzare AVG PC TuneUp per personalizzare l'aspetto del sistema Windows in base alle proprie esigenze.

### Panoramica degli stati

- Se AVG PC TuneUp non è installato, questo riquadro non è attivo (visualizzato in grigio) e il testo sottostante indica "Non ottimizzato". È tuttavia sufficiente fare clic sul riquadro per [installare questa applicazione AVG.](#)
- Se è presente un numero elevato di problemi da correggere (ad esempio quando AVG PC TuneUp è completamente disattivato), il cerchio all'interno del riquadro diventa rosso e il testo sottostante indica "Non ottimizzato". Se sono presenti solo pochi problemi di minore gravità, il cerchio all'interno del riquadro viene visualizzato in verde, ma il testo sottostante indicherà "Parzialmente ottimizzato". In entrambi i casi, verrà visualizzato un numero all'interno di un cerchio arancione (nell'angolo superiore destro del riquadro) che indica il numero di problemi che è possibile correggere. Utilizzare il [pulsante Messaggi](#) per visualizzare un elenco dei problemi ed eventualmente risolverli.
- Se non sono presenti problemi con AVG PC TuneUp, il cerchio all'interno del riquadro viene visualizzato in verde e il testo sottostante indica "Ottimizzato".

Cosa succede quando si seleziona questo riquadro:

- Se AVG PC TuneUp non è ancora stato installato, viene visualizzata una finestra di dialogo che permette di installare il prodotto AVG PC TuneUp. [Ulteriori informazioni sull'installazione dei prodotti AVG.](#)
- Quando si visualizzano i dispositivi con AVG PC TuneUp installato, si apre l'interfaccia utente di AVG PC TuneUp.
- Quando si visualizza (come [amministratore](#)) un dispositivo remoto con AVG PC TuneUp installato, si apre una finestra di dialogo con una breve panoramica dello stato di AVG PC TuneUp in tale dispositivo. Questa finestra di dialogo consente di eseguire diverse operazioni in remoto, ad esempio la manutenzione (con il pulsante **Esegui manutenzione**) o l'aggiornamento (con il pulsante



**Aggiorna**). Per accedere ad altre operazioni in remoto, fare clic sul pulsante **Mostra dettagli**, che consente di aprire la [finestra di dialogo dei messaggi](#) per i dispositivi selezionati. [Ulteriori informazioni sulla visualizzazione e la gestione dei dispositivi remoti.](#)

## HMA! PRO VPN

**Hide My Ass! Pro VPN** è un'applicazione a pagamento che consente di accedere a Internet in tutta sicurezza e in modo riservato, per proteggere i dati e visitare i siti preferiti ovunque, anche sulle reti Wi-Fi pubbliche e non protette.

### Panoramica degli stati

- Se HMA! Pro VPN non è installato, questo riquadro non è attivo (visualizzato in grigio) e il testo sottostante indica "Non installato". È tuttavia sufficiente fare clic sul riquadro per [installare questa applicazione AVG](#).
- Se HMA! Pro VPN è completamente disattivato, il cerchio all'interno del riquadro viene visualizzato in giallo e il testo sottostante indica "Disattivato".
- Se l'applicazione HMA! Pro VPN è attiva e non sono presenti problemi, il cerchio all'interno del riquadro viene visualizzato in verde e il testo sottostante indica "Attivato".

Cosa succede quando si seleziona questo riquadro:

- Se HMA! Pro VPN non è ancora stato installato, viene visualizzata una finestra di dialogo che permette di installare il prodotto. Dopo aver fatto clic sul pulsante **Ulteriori informazioni** si verrà reindirizzati alla pagina Web di AVG per acquistare il software.
- Quando si visualizza il dispositivo con HMA! Pro VPN installato, si apre l'interfaccia utente di HMA! Pro VPN.
- Quando si visualizza (come [amministratore](#)) un dispositivo remoto con questa applicazione installata, si apre una finestra di dialogo con una breve panoramica dello stato delle applicazioni in tale dispositivo. Tuttavia, questa finestra di dialogo è puramente informativa e non consente di apportare alcuna modifica. [Ulteriori informazioni sulla visualizzazione e la gestione dei dispositivi remoti.](#)

## OTTIMIZZAZIONE WEB

**AVG Web TuneUp** è un potente componente aggiuntivo del browser, completamente gratuito, che funziona con i browser Chrome, Firefox e Internet Explorer. Segnala la presenza di siti pericolosi e consente di bloccare i tracker Web invadenti (identificando i siti Web che raccolgono dati sulle attività online dell'utente). Consente inoltre di eliminare in modo semplice e rapido qualsiasi traccia delle attività eseguite online, inclusi cronologia di esplorazione e dei download e cookie.

### Panoramica degli stati

- Se AVG Web TuneUp non è installato, questo riquadro non è attivo (visualizzato in grigio) e il testo sottostante indica "Non installato". È tuttavia sufficiente fare clic sul riquadro per [installare questo componente aggiuntivo del browser offerto da AVG](#). Per alcuni browser è necessario il riavvio per completare il processo di installazione. In alcuni casi, potrebbe essere necessario consentire l'installazione direttamente nel browser.
- Se AVG Web TuneUp è completamente disattivato, il cerchio all'interno del riquadro viene visualizzato in giallo e il testo sottostante indica "Disattivato". In questo caso, è possibile utilizzare il collegamento **Apri nel browser** (oppure il [pulsante Messaggi](#)) per aprire una pagina con le istruzioni complete per l'attivazione di AVG Web TuneUp nel browser.
- Se il componente aggiuntivo del browser AVG Web TuneUp è attivo e non sono presenti problemi, il cerchio all'interno del riquadro viene visualizzato in verde e il testo sottostante indica "Attivato".





Cosa succede quando si seleziona questo riquadro:

- Se AVG Web TuneUp non è ancora stato installato, viene visualizzata una finestra di dialogo che permette di installare il prodotto AVG Web TuneUp. [Ulteriori informazioni sull'installazione dei prodotti AVG.](#)
- Quando si visualizzano i dispositivi con AVG Web TuneUp installato, si apre la panoramica del prodotto AVG Web TuneUp con l'elenco delle singole funzionalità per la privacy (**Site Safety, Do Not Track, Browser Cleaner** e **AVG Secure Search**) con l'indicazione se sono attive e in esecuzione. È anche possibile utilizzare il collegamento **Apri nel browser** per accedere all'interfaccia utente di AVG Web TuneUp nel browser Web predefinito.
- Quando si visualizza (come [amministratore](#)) un dispositivo remoto con AVG Web TuneUp installato, si apre una finestra di dialogo con una breve panoramica dello stato di AVG Web TuneUp in tale dispositivo. Questa finestra di dialogo è puramente informativa e non consente di apportare alcuna modifica. In caso di problemi che richiedono l'intervento dell'utente, è disponibile il pulsante **Mostra dettagli**, che consente di aprire la [finestra di dialogo Messaggi](#) corrispondente al dispositivo selezionato. [Ulteriori informazioni sulla visualizzazione e la gestione dei dispositivi remoti.](#)

**È possibile consultare i seguenti argomenti correlati:**

- [Come installare i prodotti AVG](#)
- [Come visualizzare e/o gestire i prodotti AVG](#)

### **2.2.1.2. Dispositivi Android**

In questo manuale vengono illustrati solamente gli aspetti relativi alla versione per PC di AVG Zen. Tuttavia, se l'utente è un [amministratore](#) è molto probabile che nella rete siano presenti anche dei dispositivi Android™. In tal caso, probabilmente si visualizzeranno contenuti differenti nei riquadri delle [categorie](#) di tali dispositivi.

#### **App AVG per dispositivi mobili attualmente disponibili:**

- **AVG AntiVirus** (gratis o a pagamento): questa app protegge da virus, malware, spyware e messaggi di testo dannosi e mantiene al sicuro i dati personali dell'utente. Questa app assicura protezione da virus e malware e offre funzionalità di scansione app in tempo reale, individuazione telefono, disattivazione attività, blocco app e cancellazione dati dal dispositivo per proteggere la privacy e l'identità online dell'utente. La scansione in tempo reale assicura la protezione da app e giochi scaricati.
- **AVG Cleaner** (gratis): consente di eseguire una pulizia rapida della cronologia del browser, delle chiamate e dei messaggi e di individuare e rimuovere dati di applicazioni indesiderati memorizzati nella cache sia dalla memoria interna del dispositivo che dalla scheda SD. Ottimizza in modo significativo lo spazio di archiviazione per migliorare e accelerare le prestazioni del dispositivo Android™.
- **AVG PrivacyFix** (gratis): questa app offre un modo semplice per gestire le impostazioni per la privacy online direttamente dal dispositivo mobile. Consente di accedere a un'unica dashboard dove è possibile visualizzare rapidamente quali informazioni si stanno condividendo e con chi su Facebook, Google e LinkedIn. Basta un semplice clic per accedere direttamente alle impostazioni da modificare. La nuova funzionalità di protezione dal tracciamento WiFi permette di preimpostare le reti WiFi note e affidabili e di bloccare il tracciamento del dispositivo nelle altre reti.

Le categorie sono le seguenti:

#### **PROTEZIONE**

Facendo clic su questo riquadro è possibile visualizzare le informazioni correlate ad **AVG AntiVirus**, tra cui scansioni e relativi risultati, oltre ad aggiornamenti delle definizioni dei virus. Come [amministratore](#) di rete, è



possibile eseguire una scansione (con il pulsante **Esegui scansione**) o un aggiornamento (con il pulsante **Aggiorna**) del dispositivo Android remoto.

## PRESTAZIONI

Facendo clic su questo riquadro è possibile visualizzare i dati relativi alle prestazioni, ovvero quali funzionalità per le prestazioni di **AVG AntiVirus** sono attive (**Disattivazione attività**, **Stato batteria**, **Piano dati**, solo per la versione a pagamento, e **Utilizzo spazio di archiviazione**) e se l'app **AVG Cleaner** è installata e in esecuzione (sono incluse anche alcune statistiche).

## PRIVACY

Facendo clic su questo riquadro è possibile visualizzare i dati relativi alla privacy, ovvero quali funzionalità per la privacy di **AVG AntiVirus** sono attive (**Blocco di applicazioni**, **Backup applicazioni** e **Blocco messaggi e chiamate**) e se l'app **AVG PrivacyFix** è installata e in esecuzione.

## ANTIFURTO

Facendo clic su questo riquadro è possibile visualizzare le informazioni relative alla funzionalità **Antifurto** di **AVG AntiVirus**, che permette di individuare il dispositivo mobile in caso di furto utilizzando Google Maps. Se nel dispositivo connesso è installata una versione a pagamento (**PRO**) di **AVG AntiVirus**, viene visualizzato anche lo stato delle funzionalità **Foto dell'utente** (che scatta una foto segreta a chiunque tenti di superare il blocco del dispositivo) e **Blocco dispositivo** (che permette all'utente di bloccare il dispositivo mobile in caso di sostituzione della scheda SIM).

**È possibile consultare i seguenti argomenti correlati:**

- [Come connettere il dispositivo mobile Android a una rete Zen esistente](#)
- [Come visualizzare e/o gestire i prodotti AVG](#)

### 2.2.1.3. Dispositivi Mac

In questo manuale vengono illustrati solamente gli aspetti relativi alla versione per PC di AVG Zen. Tuttavia, se l'utente è un [amministratore](#) è molto probabile che nella rete siano presenti anche dei dispositivi Mac. In tal caso, probabilmente si visualizzeranno contenuti differenti nei riquadri delle [categorie](#) di tali dispositivi.

#### Applicazioni AVG per Mac attualmente disponibili (solo in lingua inglese):

- **AVG AntiVirus** (gratuito) – questa potente applicazione consente di eseguire la scansione di specifici file o cartelle alla ricerca di virus e altre minacce o perfino di eseguire una scansione approfondita dell'intero sistema Mac con un solo clic. È anche disponibile una protezione in tempo reale, eseguita in modo invisibile in background. Ogni file aperto, copiato o salvato viene automaticamente esaminato senza rallentare il Mac.
- **AVG Cleaner** (gratuito) – questa applicazione consente di eliminare tutti gli elementi non necessari, come la cache e file indesiderati, la cronologia dei file scaricati, il contenuto del cestino e così via, per liberare spazio. È inoltre in grado di individuare i file duplicati sul disco rigido e di rimuovere velocemente le copie non necessarie.

Le categorie sono le seguenti:





## PROTEZIONE

Facendo clic su questo riquadro è possibile visualizzare le informazioni correlate ad **AVG AntiVirus**, tra cui scansioni e relativi risultati, oltre ad aggiornamenti delle definizioni dei virus. È anche possibile sapere se la protezione in tempo reale è attiva o meno. Come [amministratore](#) di rete, è possibile aggiornare AVG AntiVirus sul dispositivo remoto (con il pulsante **Aggiorna**) o attivare la protezione in tempo reale disattivata in precedenza (tramite la [finestra di dialogo dei messaggi](#) visualizzata facendo clic sul pulsante **Mostra dettagli**). [Ulteriori informazioni sulla visualizzazione e la gestione dei dispositivi remoti.](#)

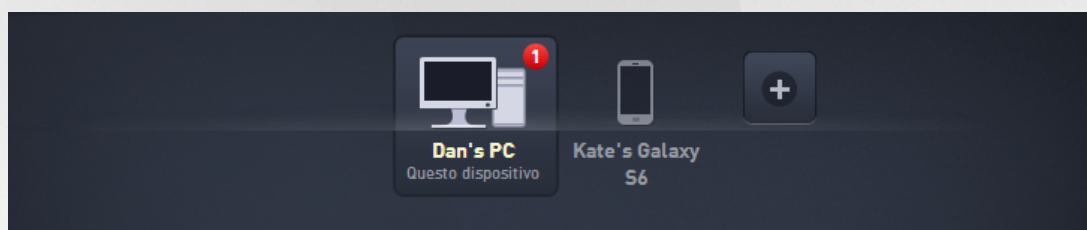
## PRESTAZIONI

Facendo clic su questo riquadro è possibile visualizzare i dati relativi alle prestazioni, ovvero i dati sui due componenti di **AVG Cleaner: Disk Cleaner e Duplicate Finder**. È possibile sapere quando è stato eseguito l'ultima volta il test con queste funzionalità per le prestazioni e quali sono stati i risultati.

**È possibile consultare i seguenti argomenti correlati:**


- [Come connettere il Mac a una rete Zen esistente](#)
- [Come visualizzare e/o gestire i prodotti AVG](#)

### 2.2.2. Area dei dispositivi



In questa parte dell'interfaccia utente di AVG Zen vengono visualizzati tutti i dispositivi disponibili nella rete Zen. Se l'utente è un [utente singolo](#), oppure è semplicemente [connesso](#) alla rete Zen di qualcun altro, visualizzerà solo il dispositivo in uso. Se invece l'utente è un [amministratore](#) di rete, il numero dei dispositivi da visualizzare potrebbe essere tale da richiedere l'utilizzo delle frecce per scorrerli tutti.

Selezionare il dispositivo da visualizzare facendo clic sul relativo riquadro. Nella [sezione delle categorie](#) verrà quindi visualizzato lo stato aggiornato dei prodotti AVG nel dispositivo selezionato. Nell'angolo superiore destro del riquadro di alcuni dispositivi potrebbe essere inoltre visualizzato un cerchio arancione con un numero. Se questo si verifica, tali dispositivi presentano alcuni problemi con i prodotti AVG che è consigliabile controllare. A tale scopo, fare clic sul [pulsante Messaggi](#) per ottenere ulteriori informazioni.

Come amministratore della rete Zen è inoltre possibile aggiungere nuovi dispositivi alla rete. A tale scopo, fare clic sul pulsante  a destra dell'area dei dispositivi. I dispositivi invitati vengono visualizzati subito nell'area dei dispositivi, ma restano inattivi (nello stato "In sospenso") finché i rispettivi utenti non accettano l'invito.

Facendo clic con il pulsante destro del mouse sui riquadri dei dispositivi è inoltre possibile aprire un menu di scelta rapida ed eseguire alcune azioni per il dispositivo selezionato:

- **Rinomina:** il nome del dispositivo nella parte inferiore del riquadro diventa editabile e può essere modificato o riscritto completamente.

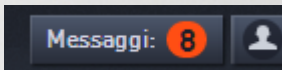


- **Modifica icona:** viene visualizzata la finestra di dialogo [Impostazioni dispositivo](#), dove è possibile scegliere una nuova icona per il dispositivo selezionato per [modificarne il tipo](#).
- **Rimuovi dalla rete:** il dispositivo selezionato verrà rimosso dalla rete Zen (verrà richiesta la conferma). *Non è possibile rimuovere il dispositivo corrente (quello in uso).*

**È possibile consultare i seguenti argomenti correlati:**

- [Come aggiungere dispositivi alla rete](#)
- [Come rimuovere i dispositivi dalla rete](#)
- [Come accettare gli inviti nella rete Zen](#)

### 2.2.3. Pulsante Messaggi

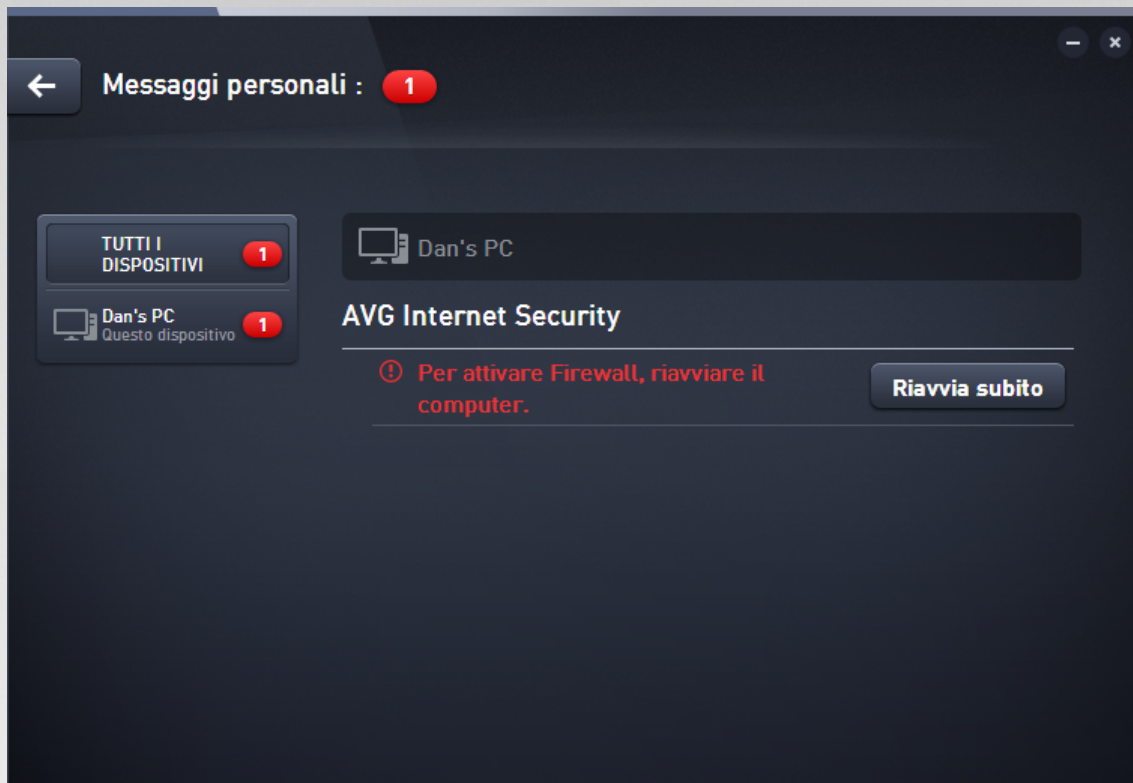


Questo pulsante è situato sopra l'[area dei dispositivi](#), a sinistra del [pulsante dello stato](#). Tuttavia, viene visualizzato solo se sono presenti problemi con i prodotti AVG nel dispositivo corrente. Nel cerchio colorato è indicato il numero di problemi che è possibile correggere.

Come [amministratore di rete](#), è inoltre possibile accedere alla **finestra di dialogo dei messaggi** per i dispositivi remoti, facendo clic sul pulsante **Mostra dettagli** (nella visualizzazione del [riquadro della categoria](#)). Questo pulsante è disponibile solo se sono presenti problemi urgenti che richiedono l'attenzione dell'utente. [Fare clic qui per leggere le informazioni su questa e altre operazioni di gestione remota.](#)

Dopo aver fatto clic su questo pulsante, verrà visualizzata una nuova finestra di dialogo:





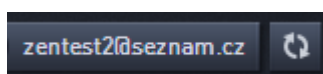
In questa finestra di dialogo è disponibile un elenco dei problemi, ordinati per categoria di prodotto. I problemi vengono visualizzati in diversi colori (rosso, giallo o blu), per distinguere i più urgenti da quelli di minore gravità.

Se l'utente è l'[amministratore](#) di una rete con più dispositivi, questa finestra di dialogo avrà un aspetto leggermente diverso. Sulla sinistra verrà visualizzata una panoramica dei dispositivi, che permette di visualizzare solo i messaggi di avviso relativi ai singoli dispositivi. Tuttavia, se si desidera visualizzare i messaggi di tutti i dispositivi in un unico elenco ordinato, è possibile selezionare l'opzione **TUTTI I DISPOSITIVI** (la prima nella parte superiore della panoramica).

Alcuni problemi possono inoltre essere gestiti direttamente dalla finestra di dialogo, tramite uno speciale pulsante di azione (denominato **Correggi ora**) visualizzato accanto ad essi. Come [amministratore](#) di rete, è possibile correggere tali problemi in remoto, direttamente da AVG Zen. Come [utente singolo](#) o [connesso](#), è possibile solo gestire i prodotti AVG sul proprio dispositivo, ma sempre senza dover aprire l'interfaccia di ciascuna applicazione (la visualizzazione di tutti i problemi insieme può risultare più pratica).

Ad esempio, quando si visualizza il testo **"RIAVVIO NECESSARIO - Per attivare Firewall, riavviare il computer."**, è possibile fare clic sul pulsante **Riavvia ora**. Il computer verrà quindi riavviato per attivare il componente Firewall.

## 2.2.4. Pulsante dello stato



Questo pulsante mostra la [modalità utente](#) in uso. Se l'utente è l'[amministratore](#) della rete Zen in genere viene visualizzato l'indirizzo email di AVG MyAccount utilizzato per connettersi alla rete.



Dopo aver fatto clic su questo pulsante, verrà visualizzato un elenco di azioni aggiuntive. Le azioni disponibili dipendono dalla [modalità utente](#) attualmente in uso:

#### Come **utente singolo**:

- **Connetti**: permette di [connettersi a una rete Zen esistente](#) (o di [crearne una nuova](#)).
- **Altre informazioni**: consente di accedere a informazioni su AVG Zen e sulla creazione di una rete Zen. Consente inoltre di accedere a una panoramica online più dettagliata.
- **Visita AVG MyAccount**: apre il browser e il sito Web <https://myaccount.avg.com/>, per consentire l'accesso al proprio AVG MyAccount.

#### Come **utente connesso**:

- **Accedi come amministratore**: questa opzione permette di ottenere i diritti di [amministratore](#) per visualizzare e gestire la rete Zen (sono necessarie le credenziali di accesso).
- **Abbandona rete**: selezionare per [abbandonare la rete Zen](#) (verrà richiesta la conferma).
- **Altre informazioni**: mostra una finestra di dialogo informativa sulla rete Zen a cui si è connessi e sul relativo amministratore.
- **Visita AVG MyAccount**: apre il browser e il sito Web <https://myaccount.avg.com/>, per consentire l'accesso al proprio AVG MyAccount.

#### Come **amministratore**:

- **Esci come amministratore**: selezionare per rinunciare ai diritti di amministratore e passare alla modalità [utente connesso](#) all'interno della stessa rete Zen.
- **Visita AVG MyAccount**: apre il browser e il sito Web <https://myaccount.avg.com/>, per consentire l'accesso al proprio AVG MyAccount.

#### Che cos'è AVG MyAccount?

AVG MyAccount è un servizio (cloud) di AVGgratuito e basato sul Web che consente di:

- visualizzare i prodotti registrati e le informazioni sulle licenze
- rinnovare facilmente la sottoscrizione e scaricare i prodotti
- controllare ordini e fatture precedenti
- gestire dati personali e password
- utilizzare AVG Zen

È possibile accedere ad AVG MyAccount direttamente dal sito Web <https://myaccount.avg.com/>.

### 2.2.4.1. Tre modalità utente

In pratica, in AVG Zen sono disponibili tre modalità utente. Il testo visualizzato nel **pulsante dello stato** dipende dalla modalità attualmente in uso:

- **Utente singolo** (il pulsante dello stato mostra **Connetti**): è appena stato installato AVG Zen. L'utente non è né amministratore di AVG MyAccount, né connesso a una rete, perciò può visualizzare e gestire solamente i prodotti AVG installati nel dispositivo in uso.
- **Utente connesso** (il pulsante dello stato mostra **Connesso**): è stato utilizzato un codice di associazione, ovvero si è [accettato un invito](#) a entrare nella rete di qualcuno. Tutti i prodotti AVG nel





dispositivo possono essere visualizzati e gestiti dall'amministratore di tale rete. L'utente può continuare a visualizzare e gestire i prodotti AVG installati nel dispositivo (come se fosse un utente singolo). Se non si desidera più far parte della rete, è possibile [abbandonarla](#).

- **Amministratore** (il pulsante dello stato mostra il **nome dell'AVG MyAccount** in uso): [si è effettuato l'accesso utilizzando AVG MyAccount](#) (oppure si è già [creato un nuovo account](#)). Ciò significa che è possibile accedere a tutte le funzionalità di AVG Zen. È possibile [aggiungere dispositivi alla rete](#), visualizzare in remoto i prodotti AVG installati e, se necessario, [rimuoverli](#) dalla rete. È anche possibile eseguire diverse [operazioni in remoto](#) nei dispositivi connessi.

#### È possibile consultare i seguenti argomenti correlati:

- [Come accettare gli inviti](#)
- [Come connettersi a una rete Zen esistente](#)
- [Come creare una nuova rete Zen network?](#)
- [Come abbandonare una rete](#)
- [Come visualizzare e/o gestire i prodotti AVG](#)

### 2.2.5. Pulsante Aggiorna / Rinnova



Facendo clic su questo pulsante (a destra del [pulsante dello stato](#)), viene aperto il negozio online AVG nel browser Web:

- Se attualmente si utilizza software AVG gratuito, ma si desiderano ulteriori funzionalità disponibili solo nelle versioni a pagamento, è possibile utilizzare il negozio per acquistare abbonamenti da 1 o 2 anni.
- Se si utilizza software AVG a pagamento, ma le sottoscrizioni stanno per scadere (o sono già scadute), è possibile utilizzare il negozio per rinnovarle.

Per attivare gli abbonamenti acquistati (o rinnovati), è necessario accedere ad [AVG MyAccount](#).

### 2.2.6. Pulsante Aggiorna



Facendo clic su questo pulsante (a destra del [pulsante Aggiorna / Rinnova](#)) è possibile aggiornare immediatamente i dati di tutti i [dispositivi](#) e le [categorie](#). Questa operazione può essere utile, ad esempio, per visualizzare i dettagli di un nuovo dispositivo aggiunto che ancora non viene mostrato nell'[area dei dispositivi](#), ma che si è certi che sia connesso.

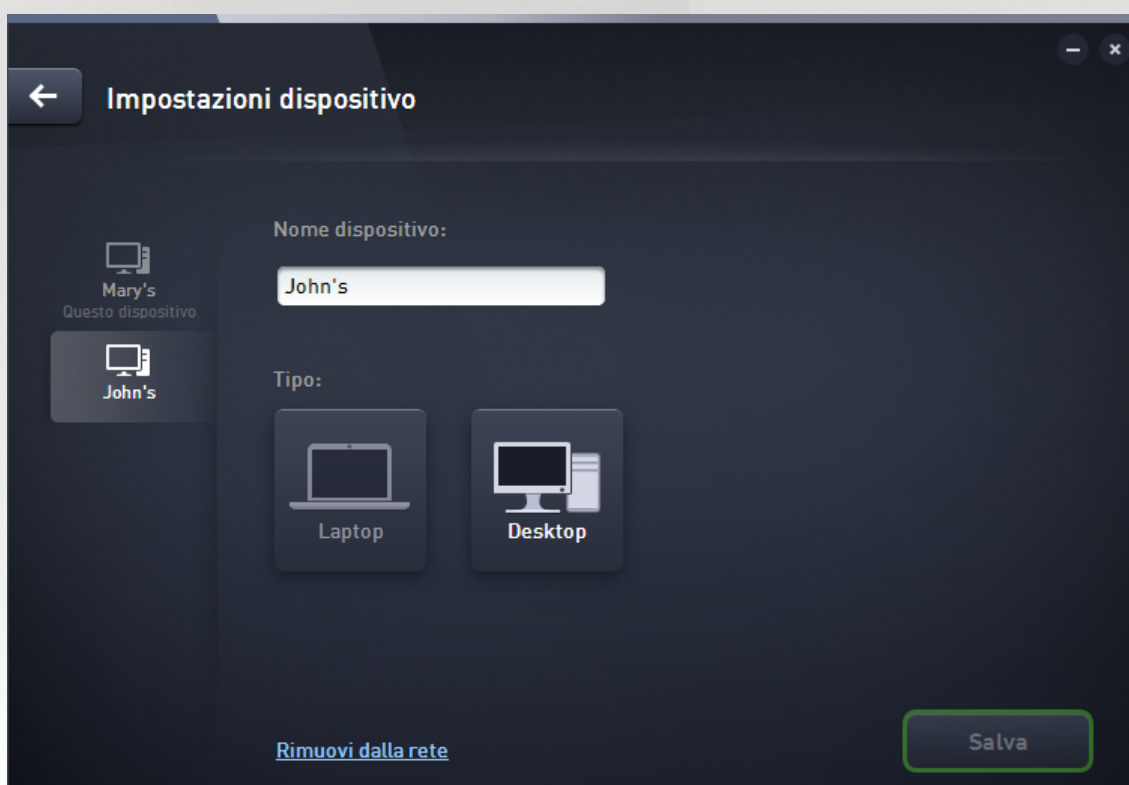


## 2.2.7. Pulsante delle impostazioni



Facendo clic su questo pulsante (a destra del pulsante [Aggiorna](#)) viene aperta una finestra popup:

- È possibile fare clic sull'opzione **Impostazioni dispositivo** per aprire la finestra di dialogo Impostazioni dispositivo, che consente di [modificare il nome e il tipo](#) per il dispositivo in uso (nonché per altri dispositivi presenti nella rete Zen, se l'utente ne è l'[amministratore](#)). In questa finestra è anche possibile [rimuovere i dispositivi dalla rete](#).



- Facendo clic sull'opzione **Assistenza in linea** si accede alla pagina Web del [Centro assistenza AVG](#), il punto di riferimento principale in caso di problemi con un prodotto AVG.
- Facendo clic su **Guida** è possibile accedere alla guida in linea del programma (è anche possibile aprire la finestra della guida in qualsiasi momento premendo il tasto **F1**).
- Infine, è possibile selezionare **Informazioni su AVG Internet Security** per visualizzare le informazioni sul software o per consultare il Contratto di licenza.

**È possibile consultare i seguenti argomenti correlati:**

- [Come modificare il nome o il tipo di dispositivo](#)
- [Come rimuovere i dispositivi dalla rete](#)







## 2.2.8. Icona dell'area di notifica

L'**icona dell'area di notifica** (disponibile sulla barra delle applicazioni di Windows, nell'angolo in basso a destra dello schermo) indica lo stato corrente di AVG Zen. È sempre disponibile nell'area di notifica, indipendentemente dall'apertura o meno dell'[interfaccia utente](#) di AVG Zen.



### Azioni accessibili tramite l'icona dell'area di notifica

È possibile fare doppio clic sull'**icona dell'area di notifica** per utilizzarla come collegamento rapido all'[interfaccia utente](#) di AVG Zen. Facendo clic con il pulsante destro del mouse sull'icona, viene aperto un menu di scelta rapida che consente di accedere ad alcune delle funzionalità più importanti:

- **Apri AVG** - utilizzare questo pulsante per aprire l'[interfaccia utente principale](#) di AVG Zen.
- **Esegui scansione** - utilizzare questo pulsante per avviare subito Scansione intero computer.
- **Protezione** (attivata  / disattivata  ) - utilizzare questo interruttore per disattivare i **AVG Internet Security** componenti che forniscono protezione in tempo reale. Sarà possibile specificare per quanto tempo **AVG Internet Security** dovrà rimanere inattivo. È inoltre possibile decidere se anche il componente Firewall deve essere disattivato. È possibile abilitare nuovamente la protezione di **AVG Internet Security** in qualsiasi momento, semplicemente facendo clic sull'interruttore.

## 2.3. Procedure dettagliate

Questo capitolo include alcune procedure dettagliate per l'esecuzione delle operazioni più comuni nell'ambiente Zen.

### 2.3.1. Come accettare gli inviti

Per chi utilizza i prodotti AVG in più dispositivi, oppure per gli utenti meno esperti che desiderano ricevere assistenza per il monitoraggio e la correzione di problemi nei prodotti AVG, è consigliabile aggiungere il PC o il dispositivo mobile Android™ a una rete Zen. Per prima cosa, tuttavia, è necessario essere invitati dall'amministratore della rete. A tale scopo, chiedere all'amministratore di inviare un messaggio email di invito. Una volta ricevuto l'invito, aprirlo e individuare il **codice di invito**.

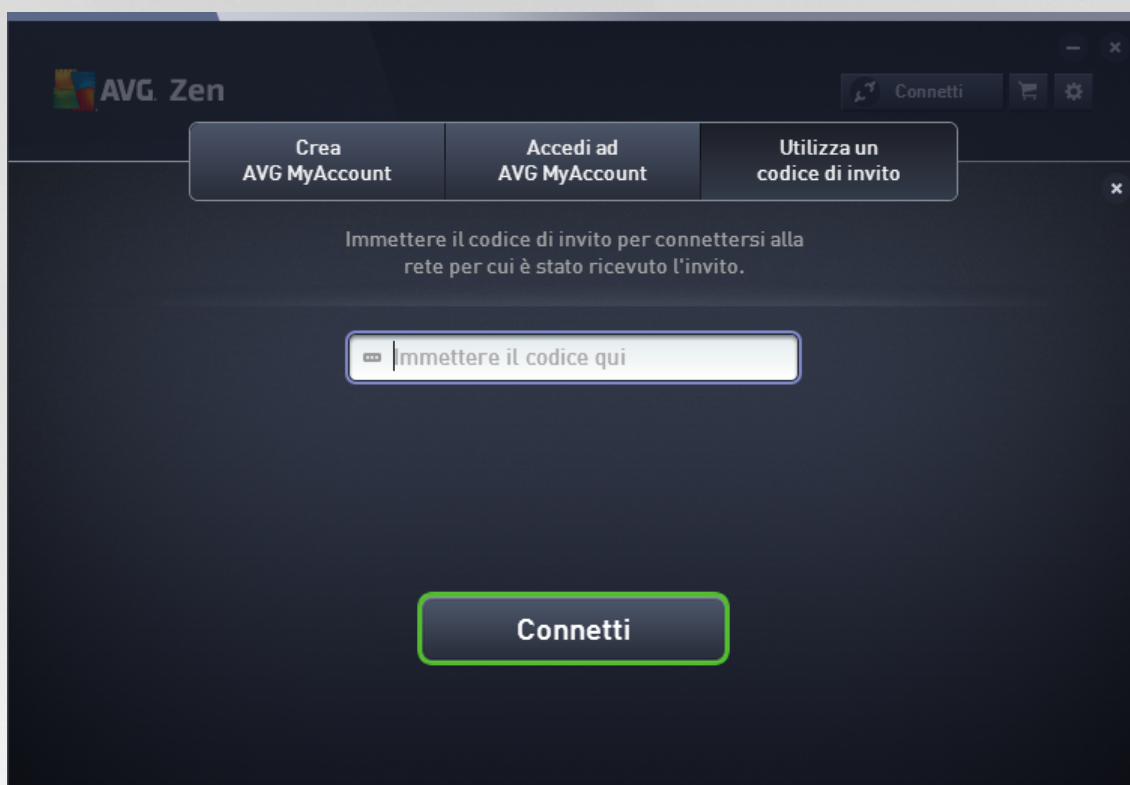
I passaggi successivi variano a seconda che si desideri aggiungere un PC o un dispositivo mobile Android™:

#### PC:

1. Se non è ancora stato installato, installare AVG Zen.



2. Fare clic sul [pulsante dello stato](#) (**Connetti**) e confermare facendo clic su **Connetti** nella finestra popup visualizzata.
3. Nella finestra di dialogo secondaria visualizzata selezionare **Utilizza un codice di invito** (ultima opzione a destra).



4. Copiare e incollare il codice di invito dal messaggio email nell'apposita casella di testo della finestra di dialogo secondaria di Zen oppure digitarlo manualmente.

Grazie alla procedura di copia e incolla è possibile inserire qualunque elemento copiabile (testi, immagini e così via) negli Appunti di Windows per poi incollarlo altrove. Il funzionamento è il seguente:

- i. Evidenziare il testo da copiare, in questo caso il codice di invito ricevuto tramite email. A tale scopo, tenere premuto il pulsante sinistro del mouse o il tasto MAIUSC.
- ii. Premere **Ctrl+C** sulla tastiera (tenere presente che in questa fase non è possibile determinare se il testo è stato effettivamente copiato).
- iii. Passare alla posizione desiderata, in questo caso la finestra di dialogo di **Zen Connettersi a una rete** e quindi fare clic nella casella in cui si desidera incollare il testo.
- iv. Premere **Ctrl+V**.
- v. Il testo incollato, ovvero il codice di invito, verrà visualizzato. Fine.

5. Fare clic sul pulsante **Connetti**. Attendere qualche istante e la connessione alla rete Zen desiderata sarà completata. Nello specifico, per l'utente cambia solo il [pulsante dello stato](#) che ora indicherà **Connesso**. Tuttavia, da questo momento il dispositivo verrà monitorato dall'amministratore della rete, che potrà identificare possibili problemi e aiutare l'utente a risolverli. In ogni caso, è possibile [abbandonare la rete](#) in qualsiasi momento.

### Dispositivi mobili Android:





Diversamente dai PC, la connessione alla rete nei dispositivi mobili Android viene eseguita direttamente dall'interno dell'applicazione:


1. Innanzitutto, è necessario che almeno un'app AVG per dispositivi mobili sia installata e connessa a una rete Zen. Fare [clic qui](#) per ulteriori informazioni sulla connessione di un dispositivo mobile Android™ a una rete Zen esistente. Per i dispositivi mobili accettare un invito significa abbandonare la rete Zen corrente per passare a un'altra.
2. Aprire l'applicazione e toccare l'**icona del menu** (ovvero il logo dell'applicazione) situata nell'angolo superiore sinistro della schermata principale.
3. Nel menu visualizzato toccare l'opzione **Gestisci dispositivi**.
4. Toccare l'opzione **Connetti a un'altra rete Zen** nella parte inferiore dello schermo, immettere il codice di invito inviato dall'amministratore della rete e quindi toccare **Connetti**.
5. Congratulazioni! Il collegamento alla rete Zen è stato completato. Tuttavia, in caso di ripensamenti, è possibile [abbandonare la rete](#) in qualsiasi momento.

### Dispositivi Mac:

Diversamente dai PC, la connessione alla rete nei dispositivi Mac viene eseguita direttamente dall'interno dell'applicazione:

1. Innanzitutto, è necessario che almeno un'applicazione AVG per Mac sia installata e possibilmente già connessa a una rete Zen. Fare [clic qui](#) per ulteriori informazioni sulla connessione di un dispositivo Mac a una rete Zen esistente. Se si è connessi, fare clic sul pulsante "Connesso" nell'angolo superiore destro della schermata dell'applicazione e scegliere **Abbandona rete** nel menu a discesa visualizzato.
2. Il pulsante nell'angolo superiore destro della schermata dell'applicazione indicherà "Non connesso". Fare clic e scegliere l'opzione **Connetti** nel menu a discesa.
3. Nella finestra di dialogo visualizzata fare clic su **Utilizza un codice di invito** (ultima opzione a destra).
4. Verrà visualizzata una casella di testo per immettere il codice di invito inviato in precedenza dall'amministratore della rete. Dopo avere immesso il codice, fare clic sul pulsante **Connetti**.
5. Congratulazioni! Il collegamento alla rete Zen è stato completato. Tuttavia, in caso di ripensamenti, è possibile [abbandonare la rete](#) in qualsiasi momento.

## 2.3.2. Come aggiungere dispositivi alla rete

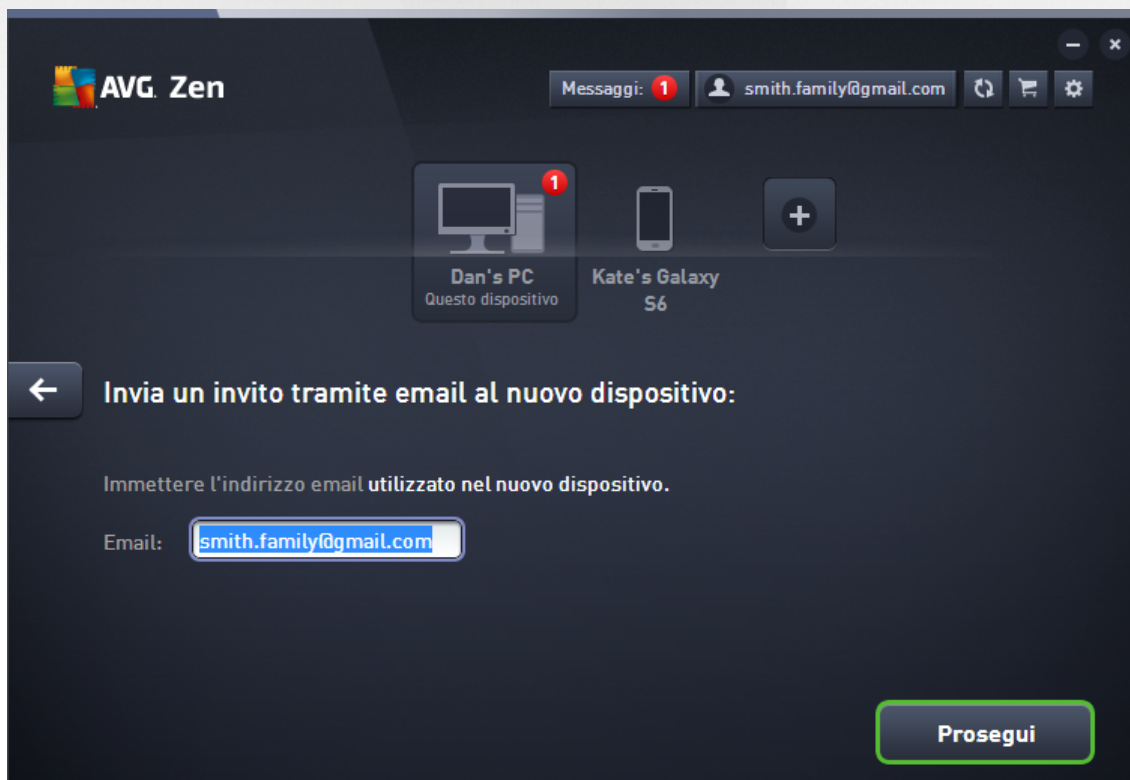
1. Per aggiungere un nuovo dispositivo alla rete Zen, è necessario invitarlo. A tale scopo, fare clic sul pulsante  a destra dell'[area dei dispositivi](#).

Tenere presente che solo gli [amministratori](#) possono inviare inviti e aggiungere dispositivi alle reti. Pertanto, se attualmente non si è connessi a nessuna rete Zen, [eseguire questa operazione](#) oppure [creare una nuova rete](#).

2. Viene visualizzata una nuova finestra di dialogo. Scegliere il tipo di dispositivo da aggiungere (ovvero PC o dispositivo mobile Android™) selezionando il riquadro appropriato e facendo clic sul pulsante **Prosegui**.



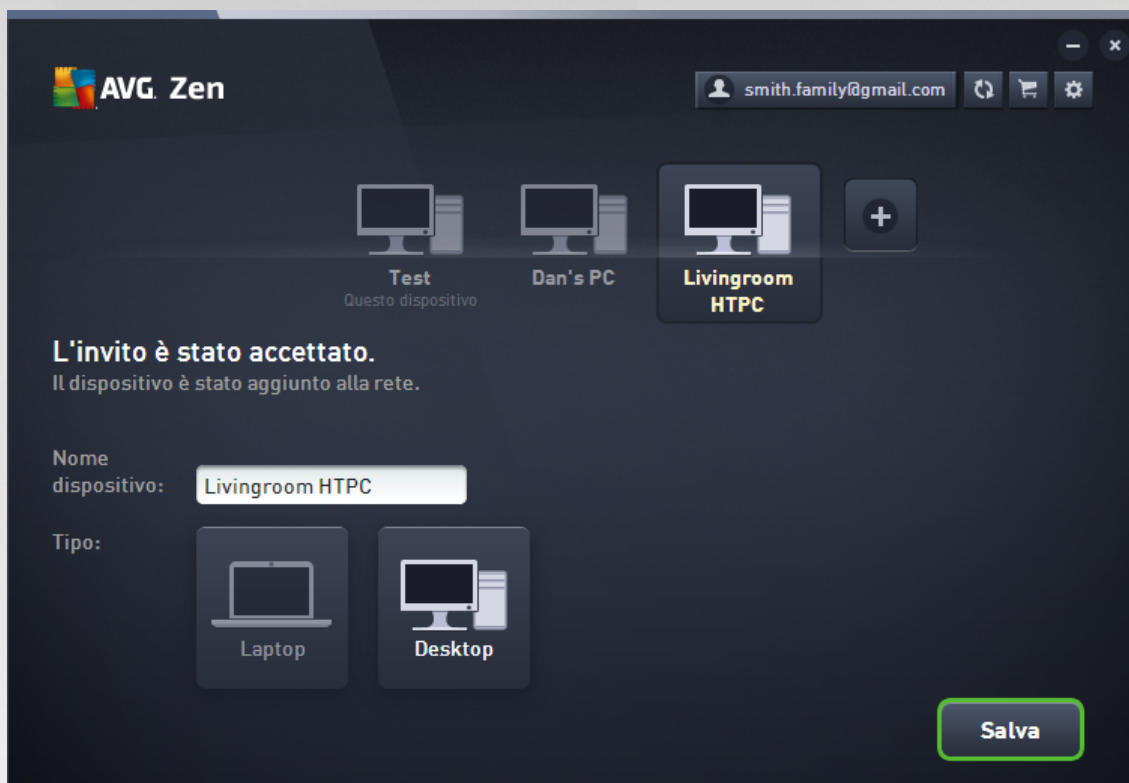
- Viene visualizzata un'altra finestra di dialogo. Immettere l'indirizzo email utilizzato nel nuovo dispositivo e fare clic sul pulsante **Prosegui**.







4. Il messaggio email di invito è stato inviato. Il dispositivo viene ora visualizzato nell'[area dei dispositivi](#) come "In sospeso". Ciò significa che l'invito è in attesa di [essere accettato](#).

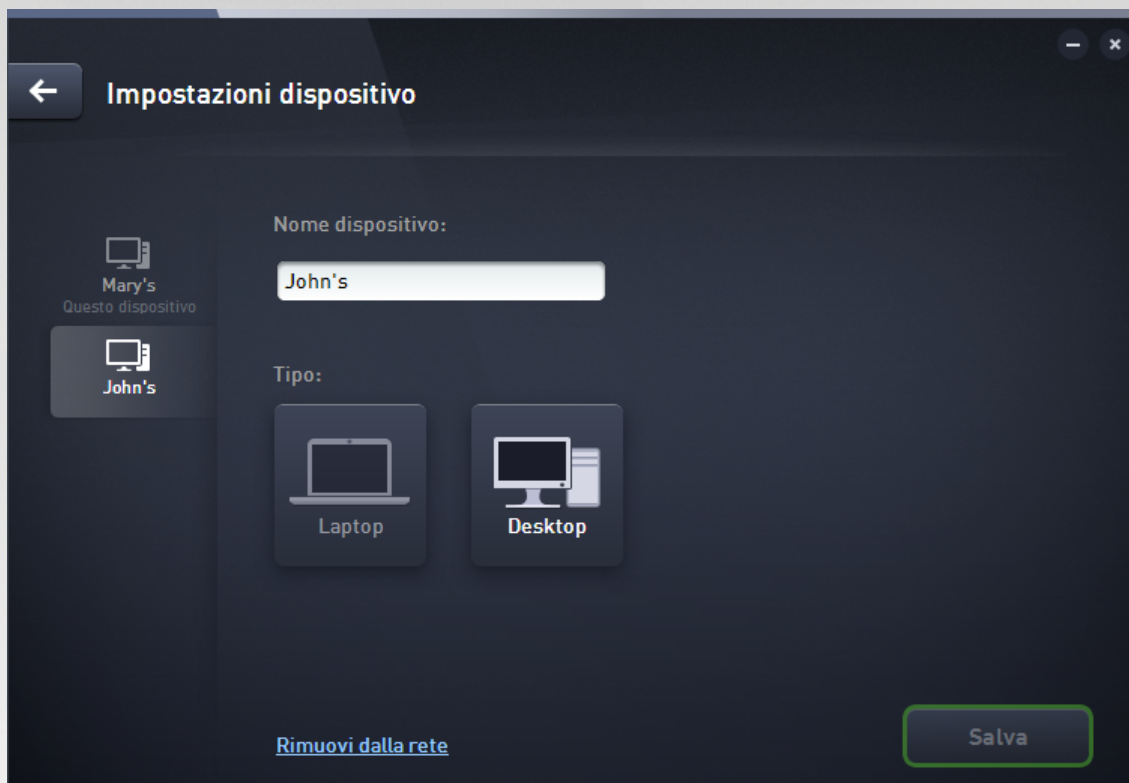


Fin tanto che l'invito rimane in sospeso, è possibile scegliere se **inviare un altro collegamento di invito** oppure **annullare l'invito** del tutto.

5. Non appena l'invito viene accettato, è possibile modificare il nome e il tipo del nuovo dispositivo (tuttavia, è possibile effettuare questa operazione anche in un secondo momento). Il dispositivo è ora parte della rete Zen ed è possibile visualizzare in remoto i prodotti AVG installati. L'utente è ora amministratore a tutti gli effetti di una rete Zen!

### 2.3.3. Come modificare il nome o il tipo di dispositivo

1. Fare clic sul [pulsante delle impostazioni](#) e selezionare **Impostazioni dispositivo** nella finestra popup.



2. Le impostazioni visualizzate sono valide per il dispositivo attualmente selezionato. Un elenco dei [dispositivi attualmente disponibili nella rete](#) (ovvero quelli che hanno accettato gli inviti) viene visualizzato in una serie di riquadri in colonna a sinistra della finestra di dialogo Impostazioni dispositivo. Fare clic sui singoli riquadri per passare da un dispositivo all'altro.
3. La casella di testo **Nome dispositivo** mostra il nome del dispositivo attualmente selezionato. È possibile cancellare il nome e sostituirlo con un altro.
4. Nella parte inferiore della finestra, è possibile impostare il **Tipo** per il dispositivo attualmente selezionato (Telefono, Tablet, Laptop o Desktop). Fare clic sul riquadro appropriato.
5. Fare clic sul pulsante **Salva** per confermare le modifiche.

È inoltre possibile fare clic con il pulsante destro del mouse su uno dei riquadri nell'[area dei dispositivi](#) e scegliere di **Rinominare** o di **Modificare l'icona** (ovvero il tipo) dal menu di scelta rapida.

### 2.3.4. Come connettersi a una rete Zen esistente

#### PC:

1. Se non si è connessi a un AVG MyAccount, fare clic sul [pulsante dello stato](#) (**Connetti**) e confermare facendo clic sull'opzione **Connetti** nella finestra popup.





Se si è già connessi a un AVG MyAccount, è necessario effettuare la disconnessione prima di connettersi a un account differente. Fare clic sul [pulsante dello stato](#) (con il nome dell'AVG MyAccount corrente) e confermare facendo clic sul pulsante **Esci** visualizzato nella finestra popup.

2. Nella finestra di dialogo secondaria visualizzata selezionare **Accedi ad AVG MyAccount** (opzione al centro).

3. Immettere il nome utente e la password di AVG MyAccount. Se non si dispone di un AVG MyAccount, è sufficiente [creare uno nuovo](#). Verrà effettuato l'accesso come [amministratore](#). Sarà pertanto possibile visualizzare i prodotti AVG nei dispositivi remoti appartenenti alla rete Zen. È possibile disconnettersi in qualsiasi momento e restare nella rete solo come [utente connesso](#).

Se non si ricorda la password, selezionare il collegamento **Password dimenticata?** sotto alla casella di testo per la password. In questo modo si verrà reindirizzati alla pagina Web per il recupero della password.

4. Fare clic sul pulsante **Accedi**. Il processo di connessione dovrebbe avvenire entro pochi secondi. Una volta stabilita la connessione, il [pulsante dello stato](#) dovrebbe visualizzare il nome dell'AVG MyAccount.

### Dispositivi mobili Android:

Diversamente dai PC, la connessione alla rete nei dispositivi mobili Android viene eseguita direttamente dall'interno dell'applicazione:

1. Per connettere un dispositivo mobile Android alla rete Zen è necessario scaricare una delle app AVG per dispositivi mobili (ovvero AVG AntiVirus, AVG Cleaner e/o AVG PrivacyFix). Questa operazione può essere effettuata utilizzando Google Play, che offre il download e l'installazione gratuita di tutte queste



applicazioni. Affinché la connessione funzioni correttamente, assicurarsi di utilizzare la versione più recente disponibile.

2. Al termine dell'installazione, aprire l'app AVG e toccare l'**icona del menu** (ovvero il logo dell'applicazione) situata nell'angolo superiore sinistro della schermata principale.
3. Nel menu visualizzato toccare l'opzione **Gestisci dispositivi**.
4. Toccare la scheda **Accesso** e immettere le credenziali di AVG MyAccount (ovvero **nome utente** e **password**).
5. Congratulazioni! Il collegamento alla rete Zen è stato completato. Selezionando l'icona del menu si dovrebbe visualizzare **Connessione effettuata come:** con il nome dell'AVG MyAccount in uso nella parte superiore del menu. Tuttavia, in caso di ripensamenti, è possibile [abbandonare la rete](#) in qualsiasi momento.

#### **Dispositivi Mac:**

Diversamente dai PC, la connessione alla rete nei dispositivi Mac viene eseguita direttamente dall'interno dell'applicazione:

1. Per connettere un dispositivo Mac alla rete Zen, è necessario scaricare una delle applicazioni AVG per Mac (ovvero AVG AntiVirus e/o AVG Cleaner). È possibile scaricare facilmente queste applicazioni, ad esempio tramite l'[Area download AVG](#) o il Mac App Store, e installarle gratuitamente. Affinché la connessione funzioni correttamente, assicurarsi di utilizzare la versione più recente disponibile.
2. Al termine dell'installazione, aprire l'applicazione AVG. Nell'angolo superiore destro della schermata dell'applicazione verrà visualizzato un pulsante di forma oblunga ("Non connesso"). Fare clic e scegliere l'opzione **Connetti** nel menu a discesa.
3. Nella finestra di dialogo visualizzata fare clic sull'opzione al centro **Accedi ad AVG MyAccount** (in genere selezionata per impostazione predefinita).
4. Immettere le credenziali di AVG MyAccount, ovvero **nome utente** (indirizzo email di AVG MyAccount) e **password**.
5. Congratulazioni! Il collegamento alla rete Zen è stato completato. Il pulsante nell'angolo superiore destro della schermata dell'applicazione indicherà "Connesso". Facendo clic su tale pulsante, è possibile sapere a quale rete si è attualmente connessi. Tuttavia, in caso di ripensamenti, è possibile [abbandonare la rete](#) in qualsiasi momento.

### **2.3.5. Come creare una nuova rete Zen**

Per creare e [amministrare](#) una nuova rete Zen, è necessario creare un AVG MyAccount personale. È possibile effettuare questa operazione in due modi: utilizzando il browser Web oppure direttamente dall'applicazione AVG Zen.

#### **Dal browser:**

1. Utilizzare il browser per aprire il sito Web <https://myaccount.avg.com/>.
2. Fare clic su **Crea il tuo AVG MyAccount**.





3. Immettere l'indirizzo email di accesso, impostare una password, digitare nuovamente la password e fare clic sul pulsante **Crea account**.
4. Si riceverà un collegamento per l'attivazione di AVG MyAccount (all'indirizzo email utilizzato nel passaggio 3). È necessario fare clic sul collegamento per completare la creazione di AVG MyAccount. Se non viene visualizzato nella posta in arrivo, il messaggio potrebbe essere stato spostato nella cartella dello spam.

#### A partire da AVG Zen:

1. Se non si è attualmente connessi a un AVG MyAccount, fare clic sul [pulsante dello stato](#) (**Connetti**) e confermare facendo clic sull'opzione **Connetti** nella finestra popup.

Se si è già connessi a un AVG MyAccount, è necessario effettuare la disconnessione prima di connettersi a un account differente. Fare clic sul [pulsante dello stato](#) (con il nome dell'AVG MyAccount corrente) e confermare facendo clic sul pulsante **Esci** visualizzato nella finestra popup.

2. Nella finestra di dialogo secondaria visualizzata assicurarsi che **Crea il tuo AVG MyAccount** sia selezionato (in genere selezionata per impostazione predefinita).

3. Immettere l'indirizzo email di accesso, impostare una password, quindi fare clic sul pulsante **Crea account**.
4. Dopo qualche secondo, si verrà connessi alla nuova rete con i diritti di [amministratore](#). Sarà pertanto possibile [aggiungere dispositivi alla rete](#), visualizzare in remoto i prodotti AVG installati e, se necessario, [rimuoverli](#) dalla rete. È possibile disconnettersi in qualsiasi momento e restare nella rete solo come [utente connesso](#).



## 2.3.6. Come installare i prodotti AVG

1. I prodotti AVG possono essere installati rapidamente tramite Zen. A tale scopo, fare clic sul riquadro di una [categoria](#) (il cerchio all'interno del riquadro viene visualizzato in grigio se non è disponibile alcun prodotto per tale categoria oppure in verde per metà se è già stato installato un prodotto, ma è possibile installarne un altro).



2. Per avviare l'installazione del prodotto, è sufficiente fare clic sul pulsante **Download GRATUITO**. Il prodotto verrà quindi installato automaticamente con le impostazioni predefinite.

Per personalizzare il processo di installazione, fare clic sulla freccia (a destra del pulsante **Download GRATUITO**) e selezionare **Installazione personalizzata**. In questo modo, l'installazione verrà visualizzata come una serie di finestre di dialogo, per consentire all'utente di modificare la cartella di destinazione, i componenti installati e così via.

Il processo di installazione per i vari prodotti AVG è descritto in dettaglio nell'altra parte della documentazione o in manuali per l'utente distinti. Tali manuali possono essere facilmente scaricati dal [sito Web di AVG](#).

3. Man mano che l'installazione procede, il cerchio all'interno del riquadro della [categoria](#) selezionata dovrebbe diventare verde. Al termine dell'installazione, il cerchio verde all'interno del riquadro è completo (in alcune categorie potrebbe essere visualizzato solo un semicerchio, se è possibile installare altri prodotti per quella categoria). Tenere presente che il cerchio (o semicerchio) potrebbe cambiare colore (giallo o rosso) immediatamente dopo l'installazione. Ciò significa che sono presenti problemi con il relativo prodotto che richiedono l'attenzione dell'utente.
4. Si riceverà un messaggio di conferma (visualizzato sotto i riquadri delle [categorie](#)) dell'avenuta





installazione.

### 2.3.7. Come abbandonare una rete

#### PC:

1. Le operazioni da eseguire per uscire da una rete Zen a cui si è connessi sono molto semplici. Per prima cosa, fare clic sul [pulsante dello stato](#) (con il testo **Connesso**) e selezionare il pulsante **Abbandona rete** nella finestra popup per proseguire.
2. Ora è necessario confermare che si desidera abbandonare la rete Zen. A tale scopo, fare clic sul pulsante **Abbandona**.
3. In pochi secondi, si verrà disconnessi in modo permanente. L'amministratore non sarà più in grado di gestire i prodotti AVG nel PC dell'utente che ha abbandonato la rete. Nel [pulsante dello stato](#) verrà visualizzato il testo **Connetti** (ovvero tornerà allo stato iniziale).

#### Dispositivi mobili Android:

Diversamente dai PC, la connessione alla rete nei dispositivi mobili Android viene eseguita direttamente dall'interno dell'applicazione:

1. Aprire l'app AVG e toccare **l'icona del menu** (ovvero il logo dell'applicazione) situata nell'angolo superiore sinistro della schermata principale.
2. Proprio sopra il menu, si dovrebbe visualizzare il testo **Connessione effettuata come:**, insieme al nome dell'AVG MyAccount in uso. Subito accanto, è disponibile una icona a forma di porta con una freccia puntata verso destra. Fare clic sull'icona.
3. Confermare che si desidera abbandonare la rete Zen facendo clic sul pulsante **OK**.
4. In pochi secondi, si verrà disconnessi in modo permanente. L'amministratore non sarà più in grado di gestire i prodotti AVG nel dispositivo mobile Android™ dell'utente che ha abbandonato la rete. Tuttavia, è possibile connettersi nuovamente a questa (o a qualsiasi altra) rete Zen [direttamente](#) o [accettando un invito](#).

#### Dispositivi Mac:

Diversamente dai PC, la connessione alla rete nei dispositivi Mac viene eseguita direttamente dall'interno dell'applicazione:

1. Aprire l'applicazione AVG e fare clic sul pulsante oblungo nell'angolo superiore destro della schermata dell'applicazione (con il testo "Connesso").
2. Proprio sopra il menu a discesa, si dovrebbe visualizzare il testo **Connessione effettuata alle seguenti reti Zen;**, insieme al nome dell'AVG MyAccount in uso.
3. Sotto le informazioni sulla rete Zen, è disponibile un'opzione **Abbandona rete**. Fare clic sull'icona.
4. In pochi secondi, si verrà disconnessi in modo permanente. L'amministratore non sarà più in grado di gestire i prodotti AVG nel dispositivo Mac dell'utente che ha abbandonato la rete. Tuttavia, è possibile connettersi nuovamente a questa (o a qualsiasi altra) rete Zen [direttamente](#) o [accettando un invito](#).



### 2.3.8. Come rimuovere i dispositivi dalla rete

1. Le operazioni per eliminare un dispositivo dalla rete Zen sono molto semplici. Fare clic sul [pulsante delle impostazioni](#) e quindi selezionare **Impostazioni dispositivo** nella finestra popup.
2. A sinistra della finestra di dialogo Impostazioni dispositivo sono elencati i [dispositivi attualmente presenti nella rete](#), in una serie di riquadri in colonna. Passare al dispositivo da rimuovere facendo clic sul riquadro con il relativo nome.
3. Sul bordo inferiore della finestra di dialogo è visualizzato il collegamento **Rimuovi dalla rete**. Fare clic sul collegamento.

Tenere presente che non esiste un'opzione equivalente nelle impostazioni per il dispositivo che si sta utilizzando. Tale dispositivo viene considerato come il nucleo della rete e perciò non può essere rimosso.

4. Ora è necessario confermare la rimozione del dispositivo dalla rete Zen. A tale scopo, fare clic sul pulsante **Rimuovi**.
5. In pochi istanti, il dispositivo verrà rimosso in modo permanente. Non sarà più possibile gestire i prodotti AVG del dispositivo rimosso, che non verrà più visualizzato nell'[area dei dispositivi](#) dell'interfaccia utente.

Per rimuovere un dispositivo è anche possibile fare clic con il pulsante destro del mouse sul relativo riquadro nell'[area dei dispositivi](#) e scegliere **Rimuovi dalla rete** dal menu di scelta rapida. Per confermare l'operazione, fare clic sul pulsante **Rimuovi**.

### 2.3.9. Come visualizzare e/o gestire i prodotti AVG

#### Per visualizzare e gestire il dispositivo in uso

È sufficiente fare clic sul riquadro della [categoria](#) appropriata. In questo modo viene aperta l'interfaccia utente del prodotto AVG, che permette di esplorare e modificare la configurazione in base alle esigenze. Ad esempio, facendo clic sul riquadro **PROTEZIONE** si apre l'interfaccia utente di AVG Internet Security e così via. Se una categoria include più prodotti, è necessario fare clic sul riquadro e poi selezionare il riquadro secondario appropriato (ad esempio AVG PrivacyFix nella categoria **PRIVACY E IDENTITÀ**).

I prodotti AVG che possono essere visualizzati e gestiti tramite Zen sono descritti in dettaglio nell'altra parte della documentazione o in manuali per l'utente distinti. Per scaricare questi manuali, visitare il [sito Web di AVG](#).

Nel caso in cui siano presenti problemi urgenti che richiedono l'attenzione dell'utente, è possibile fare clic sul [pulsante Messaggi](#). La nuova finestra di dialogo contiene un elenco dei problemi riscontrati, alcuni dei quali possono essere corretti direttamente dalla finestra stessa tramite uno speciale pulsante di azione visualizzato in corrispondenza.

#### Se si desidera visualizzare e gestire un dispositivo remoto (solo amministratori)

Anche questa operazione è piuttosto semplice. Scegliere il dispositivo da visualizzare dall'[area dei dispositivi](#) e fare clic su un [riquadro di categoria](#) appropriato. A questo punto viene visualizzata una nuova finestra di dialogo, che include una breve panoramica degli stati dei prodotti AVG per questa categoria.





Come [amministratore](#), è possibile utilizzare diversi pulsanti per eseguire molte operazioni in remoto sui prodotti AVG nella rete Zen. Le operazioni disponibili dipendono dal tipo di dispositivo ([PC](#), [Android](#) o [Mac](#)) e dal [riquadro della categoria](#) visualizzato. Alcune operazioni (ad esempio la scansione o l'aggiornamento) potrebbero non essere accessibili se sono state già eseguite di recente. Di seguito sono elencate tutte le operazioni disponibili in remoto per i prodotti AVG:

TIPO DI DISPOSITIVO	RIQUADRO DELLA CATEGORIA	OPERAZIONI DISPONIBILI IN REMOTO
PC	<b>PROTEZIONE (AVG Internet Security)</b>	<ul style="list-style-type: none"> <li>• Pulsante <b>Esegui scansione</b>: facendo clic sul pulsante, si avvia immediatamente la scansione del dispositivo remoto per rilevare virus e altri software dannosi. Al termine della scansione verranno visualizzati i risultati. Fare clic qui per ulteriori informazioni sulla scansione in AVG Internet Security.</li> <li>• Pulsante <b>Aggiorna</b>: facendo clic sul pulsante, si avvia il processo di aggiornamento di AVG Internet Security nel dispositivo remoto. Tutte le applicazioni antivirus devono essere mantenute aggiornate per assicurare il massimo livello di protezione. Fare clic qui per ulteriori informazioni sull'importanza degli aggiornamenti in AVG Internet Security.</li> <li>• Pulsante <b>Mostra dettagli</b>: questo pulsante è disponibile solo se</li> </ul>

TIPO DI DISPOSITIVO	RIQUADRO DELLA CATEGORIA	OPERAZIONI DISPONIBILI IN REMOTO
		<p>sono presenti problemi urgenti che richiedono l'attenzione dell'utente. Facendo clic sul pulsante, si apre la <a href="#">finestra di dialogo dei messaggi</a> per il dispositivo attualmente selezionato. In questa finestra di dialogo è disponibile un elenco dei problemi, ordinati per categoria di prodotto. Alcuni di questi problemi possono essere risolti subito facendo clic sul pulsante <b>Correggi ora</b>. In AVG Internet Security, ad esempio, è possibile attivare i componenti di protezione disattivati in precedenza.</p>
PC	<b>PRESTAZIONI</b> (AVG PC TuneUp)	<ul style="list-style-type: none"> <li>• Pulsante <b>Esegui manutenzione</b>: facendo clic sul pulsante, si avvia la manutenzione del sistema (un insieme di attività per pulire il sistema nel dispositivo remoto, velocizzarlo e ottimizzare le prestazioni).</li> <li>• Pulsante <b>Aggiorna</b>: facendo clic sul pulsante, si avvia il processo di aggiornamento di AVG PC TuneUp sul dispositivo remoto. È molto importante mantenere aggiornato AVG PC TuneUp, poiché le funzionalità vengono continuamente estese o adattate per adeguarsi alle tecnologie più recenti e gli errori vengono corretti.</li> <li>• Pulsante <b>Mostra dettagli</b>: questo pulsante è disponibile solo se sono presenti problemi urgenti che richiedono l'attenzione dell'utente. Facendo clic sul pulsante, si apre la <a href="#">finestra di dialogo dei messaggi</a> per il dispositivo attualmente selezionato. In questa finestra di dialogo è disponibile un elenco dei problemi, ordinati per categoria di prodotto. Alcuni di questi problemi possono essere risolti subito facendo clic sul pulsante <b>Correggi ora</b>.</li> </ul>
Android	<b>PROTEZIONE</b> (AVG AntiVirus)	<ul style="list-style-type: none"> <li>• Pulsante <b>Esegui scansione</b>: facendo clic sul pulsante, si avvia immediatamente la scansione del dispositivo Android remoto per rilevare virus e altri contenuti dannosi. Al termine della scansione verranno visualizzati i risultati.</li> <li>• Pulsante <b>Aggiorna</b>: facendo clic sul pulsante, si avvia il processo di aggiornamento di AVG AntiVirus sul dispositivo Android remoto. Tutte le applicazioni antivirus devono essere mantenute aggiornate per assicurare il massimo livello di protezione.</li> <li>• Pulsante <b>Mostra dettagli</b>: questo pulsante è disponibile solo se sono presenti problemi urgenti che richiedono l'attenzione dell'utente. Facendo clic sul pulsante, si apre la <a href="#">finestra di dialogo dei messaggi</a> per il dispositivo attualmente selezionato. In questa finestra di dialogo è disponibile un elenco dei problemi, ordinati per categoria di prodotto. Tuttavia, in AVG AntiVirus per Android questa finestra di dialogo è esclusivamente informativa e non è possibile modificarne le impostazioni.</li> </ul>





TIPO DI DISPOSITIVO	RIQUADRO DELLA CATEGORIA	OPERAZIONI DISPONIBILI IN REMOTO
Mac	<b>PROTEZIONE (AVG AntiVirus)</b>	<ul style="list-style-type: none"> <li>• Pulsante <b>Aggiorna</b>: facendo clic sul pulsante, si avvia il processo di aggiornamento di AVG AntiVirus sul dispositivo Mac remoto. Tutte le applicazioni antivirus devono essere mantenute aggiornate per assicurare il massimo livello di protezione.</li> <li>• Pulsante <b>Mostra dettagli</b>: questo pulsante è disponibile solo se sono presenti problemi urgenti che richiedono l'attenzione dell'utente. Facendo clic sul pulsante, si apre la <a href="#">finestra di dialogo dei messaggi</a> per il dispositivo attualmente selezionato. In questa finestra di dialogo è disponibile un elenco dei problemi, ordinati per categoria di prodotto. Per AVG AntiVirus per Mac è possibile utilizzare il pulsante <b>Correggi ora</b> per attivare la protezione in tempo reale disattivata in precedenza.</li> </ul>

## 2.4. Domande frequenti e assistenza

È possibile accedere rapidamente e in qualsiasi momento all'assistenza per gli utenti di AVG Zen facendo clic sul [pulsante delle impostazioni](#) e quindi scegliendo l'opzione **Assistenza**.

Nel browser viene visualizzata la pagina del [Centro assistenza AVG](#). Questa pagina consente di accedere all'assistenza utenti degli esperti AVG. È possibile porre domande riguardo a licenze, installazione, virus e funzionalità specifiche dei prodotti. Si tratta del punto di riferimento principale in caso di problemi con un prodotto AVG.

Se invece si desidera ottenere maggiori informazioni su AVG Zen, visitare il sito di [www.avg.com/zen](http://www.avg.com/zen).

Se la connessione a Internet non è disponibile e si riscontrano problemi durante la riconnessione, contattare il provider Internet per ricevere assistenza. Senza la connessione a Internet, AVG Zen non funzionerà correttamente e non sarà possibile utilizzare neanche le opzioni di assistenza.



## 3. AVG Internet Security

Questa sezione del manuale per l'utente fornisce la documentazione completa relativa a **AVG Internet Security**.

Sono tuttavia disponibili anche altre fonti di informazioni:

- **File della Guida:** una sezione *Risoluzione dei problemi* è disponibile direttamente nel file della Guida incluso in **AVG Internet Security** (per aprire il file della Guida, premere il tasto *F1* in qualsiasi finestra di dialogo nell'applicazione). Questa sezione fornisce un elenco delle situazioni che con maggiore frequenza spingono un utente a ricercare assistenza professionale per un problema tecnico. Selezionare la situazione che descrive meglio il problema corrente e fare clic sul collegamento per aprire le istruzioni dettagliate per la risoluzione del problema.
- **Centro di assistenza del sito Web di AVG:** in alternativa, è possibile ricercare la soluzione al problema nel sito Web di AVG (<http://www.avg.com>). Nella sezione **Centro di assistenza** è disponibile una panoramica strutturata di gruppi tematici che trattano problemi commerciali e tecnici.
- **Domande frequenti:** sul sito Web di AVG (<http://www.avg.com>) è inoltre disponibile un'ampia sezione separata di domande frequenti. Questa sezione è accessibile tramite l'opzione di menu **Centro di assistenza / Domande frequenti e tutorial**. Anche in questo caso, tutte le domande sono suddivise chiaramente nelle categorie commerciale, tecnica e virus.
- **AVG ThreatLabs:** un sito Web specifico correlato ad AVG (<http://www.avgthreatlabs.com/website-safety-reports/>) dedicato ai virus, che fornisce una panoramica strutturata delle informazioni relative alle minacce online. Sono inoltre disponibili istruzioni sulla rimozione di virus e spyware e consigli relativi alla protezione.
- **Forum di discussione:** è inoltre possibile utilizzare il forum di discussione degli utenti AVG disponibile all'indirizzo <http://forums.avg.com>.





## 3.1. Processo di installazione di AVG

Per installare **AVG Internet Security** nel computer è necessario disporre del file di installazione più recente. Per assicurarsi di installare la versione aggiornata di **AVG Internet Security**, si consiglia di scaricare il file di installazione dal sito Web di AVG (<http://www.avg.com/>). La sezione **Centro di assistenza** fornisce una panoramica strutturata dei file di installazione per ciascuna edizione di AVG. Dopo aver scaricato e salvato il file di installazione sul disco rigido, è possibile avviare il processo di installazione. L'installazione è una sequenza di finestre di dialogo semplici e chiare. Ciascuna finestra di dialogo descrive brevemente come procedere in ciascuna fase del processo di installazione. Di seguito viene fornita una descrizione dettagliata di ciascuna finestra di dialogo:

### 3.1.1. Finestra introduttiva

Il processo di installazione comincia con la finestra di dialogo **Benvenuti in AVG Internet Security**.



#### Selezione lingua

In questa finestra di dialogo è possibile selezionare la lingua utilizzata per il processo di installazione. Fare clic sulla casella combinata accanto all'opzione **Lingua** per visualizzare il menu a discesa della lingua. Selezionare la lingua desiderata. Il processo di installazione procederà quindi nella lingua prescelta. Anche l'applicazione comunicherà nella lingua selezionata, con la possibilità di passare all'inglese (opzione installata per impostazione predefinita).

#### Contratto di licenza con l'utente finale e Informativa sulla privacy

Prima di proseguire con il processo di installazione, si consiglia di leggere il **Contratto di licenza con l'utente finale** e l'**Informativa sulla privacy**. È possibile accedere a entrambi i documenti tramite i collegamenti disponibili nella parte inferiore della finestra di dialogo. Fare clic su uno dei collegamenti ipertestuali per aprire una nuova finestra di dialogo / finestra del browser dove è disponibile il testo completo del rispettivo documento. Si consiglia di leggere con attenzione questi documenti, poiché sono legalmente vincolanti. Fare clic sul pulsante **Prosegui** per confermare l'accettazione dei documenti.



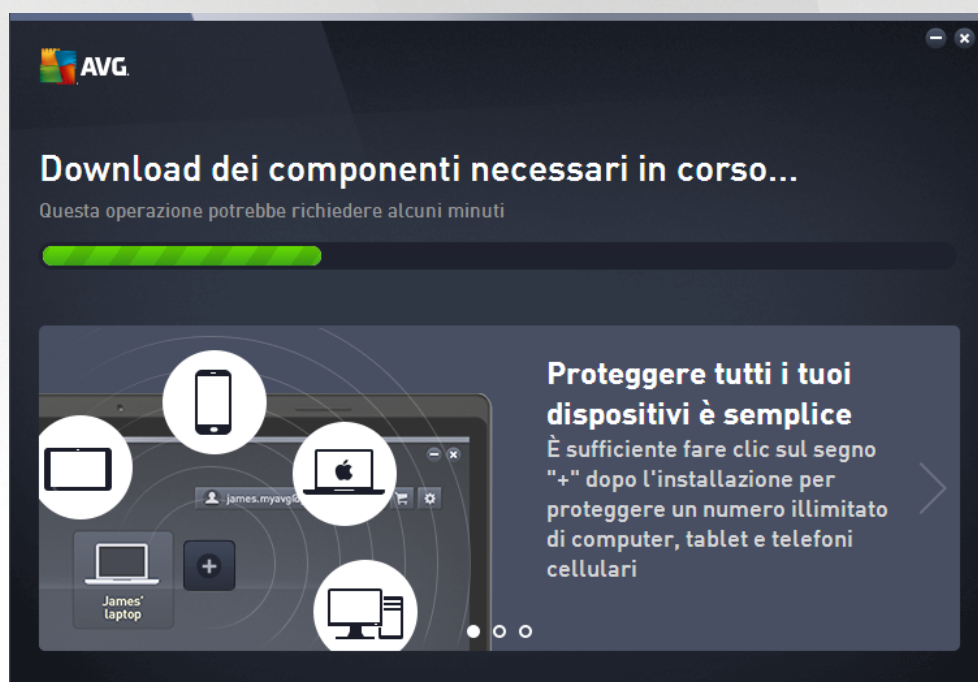
### Proseguire con l'installazione

Per proseguire con l'installazione, fare clic sul pulsante **Prosegui**. Viene richiesto di indicare il License Number, quindi il processo di installazione procede in modalità completamente automatica. Alla maggior parte degli utenti si consiglia di mantenere selezionata l'opzione per l'installazione standard di **AVG Internet Security** con tutte le impostazioni predefinite dal produttore del software. Questa configurazione fornisce la massima protezione combinata con l'utilizzo ottimale delle risorse. In futuro, se ci fosse necessità di modificare la configurazione, sarà possibile farlo direttamente nell'applicazione.

In alternativa è possibile scegliere l'opzione **Installazione personalizzata**, utilizzando il collegamento ipertestuale disponibile sotto al pulsante **Prosegui**. L'installazione personalizzata deve essere utilizzata solo da utenti esperti che hanno valide ragioni per installare l'applicazione con impostazioni non standard, ad esempio per soddisfare requisiti di sistema specifici. Se si decide di utilizzare questo tipo di installazione, immettere il License Number per visualizzare la finestra di dialogo **Personalizza l'installazione**, dove è possibile specificare le impostazioni desiderate.

## 3.1.2. Installazione di AVG

Dopo avere confermato l'avvio dell'installazione nella finestra di dialogo precedente, il processo di installazione viene eseguito in modalità completamente automatica e non richiede alcun intervento:



Al termine dell'installazione, verrà richiesto di creare un account di rete. Per informazioni dettagliate, vedere il capitolo **Come creare una nuova rete Zen?**

## 3.2. Dopo l'installazione

### 3.2.1. Aggiornamento del database dei virus

Tenere presente che, al momento dell'installazione (*dopo il riavvio del computer, se necessario*), **AVG Internet Security** aggiorna automaticamente il database dei virus e tutti i componenti e li rende completamente operativi. Questa operazione può richiedere alcuni minuti. Mentre è in corso il processo di installazione, si





riceverà una notifica dalle informazioni visualizzate nella finestra di dialogo principale. Al termine del processo di aggiornamento, la protezione di **AVG Internet Security** sarà completamente attiva e funzionante.

### 3.2.2. Registrazione del prodotto

Al termine dell'installazione di **AVG Internet Security**, registrare il prodotto in linea nel sito Web di AVG (<http://www.avg.com>). Dopo la registrazione sarà possibile ottenere l'accesso completo all'account utente AVG, alla newsletter di aggiornamento AVG e ad altri servizi offerti esclusivamente agli utenti registrati. Il modo più facile per effettuare la registrazione è quello di procedere direttamente dall'interfaccia utente di **AVG Internet Security**. Nel menu di spostamento superiore, selezionare la voce [Opzioni / Registra ora](#). Si verrà reindirizzati alla pagina della **registrazione** del sito Web di AVG (<http://www.avg.com>). Seguire le istruzioni fornite nella pagina.

### 3.2.3. Accesso all'interfaccia utente

È possibile accedere alla [finestra di dialogo principale di AVG](#) in diversi modi:

- tramite doppio clic sull'icona dell'area di notifica di AVG Internet Security
- tramite doppio clic sull'icona di AVG Protection sul desktop
- dal menu *Start / Tutti i programmi / AVG / AVG Protection*

### 3.2.4. Scansione dell'intero computer

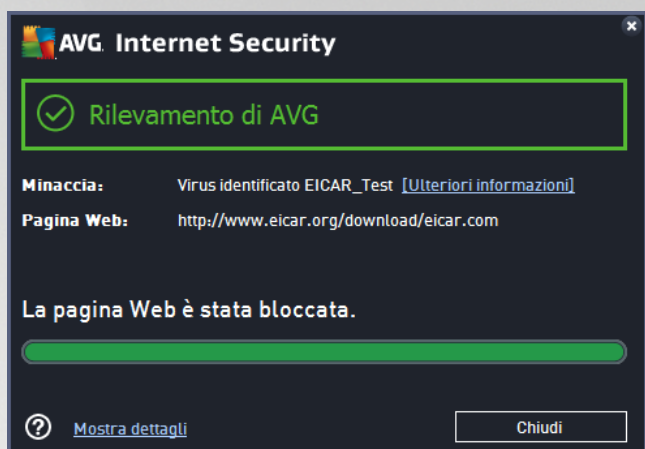
Esiste il rischio potenziale che un virus sia stato trasmesso al computer dell'utente prima dell'installazione di **AVG Internet Security**. Per questo motivo è necessario eseguire [Scansione intero computer](#) per assicurarsi che non siano presenti infezioni sul PC. La prima scansione potrebbe richiedere diverso tempo (*circa un'ora*), ma si consiglia di eseguirla comunque per verificare che il computer non sia stato compromesso da una minaccia. Per istruzioni sull'esecuzione di [Scansione intero computer](#), consultare il capitolo [Scansione AVG](#).

### 3.2.5. Controllo Eicar

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

Il controllo EICAR è un metodo standard e assolutamente sicuro per verificare il funzionamento del sistema antivirus. La sua esecuzione è sicura perché non si tratta di un vero virus e non include frammenti del codice di qualche virus. La maggior parte dei prodotti reagisce a questo controllo come se fosse un virus *anche se normalmente lo segnalano con un nome ovvio come "EICAR-AV-Test"*. È possibile scaricare il virus EICAR dal sito Web di EICAR all'indirizzo [www.eicar.com](http://www.eicar.com), in cui si troveranno anche tutte le informazioni necessarie sul controllo EICAR.

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



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

### 3.2.6. Configurazione predefinita di AVG

La configurazione predefinita (ovvero la modalità di impostazione dell'applicazione dopo l'installazione) di **AVG Internet Security** è impostata dal fornitore del software in modo che tutti i componenti e le funzioni siano ottimizzati per offrire il massimo delle prestazioni. **A meno che non esista un motivo valido per farlo, si consiglia di non modificare la configurazione di AVG! Le modifiche alle impostazioni dovrebbero essere eseguite solo da un utente esperto.** Se si desidera modificare la configurazione di AVG per adeguare l'applicazione alle proprie esigenze, accedere a [Impostazioni AVG avanzate](#): selezionare la voce del menu principale *Opzioni/Impostazioni avanzate* e modificare la configurazione di AVG nella finestra di dialogo [Impostazioni AVG avanzate](#) visualizzata.

## 3.3. Interfaccia utente di AVG

AVG Internet Security apre con la finestra principale:







La finestra principale è suddivisa in diverse sezioni:

- **Menu di spostamento superiore:** è costituito dai quattro collegamenti attivi nella sezione superiore della finestra principale (*Altro da AVG, Rapporti, Supporto, Opzioni*). [Dettagli >>](#)
- **Informazioni sullo stato di protezione:** fornisce informazioni di base sullo stato corrente di **AVG Internet Security**. [Dettagli >>](#)
- **Pulsante Vai a Zen:** consente di aprire l'interfaccia utente principale dell'applicazione ZEN, dove è possibile gestire in modo centralizzato la protezione, le prestazioni e la privacy di tutti i dispositivi utilizzati.
- **Panoramica dei componenti installati:** facendo clic sui riquadri al centro della finestra principale è possibile accedere ai vari componenti. I componenti vengono visualizzati come blocchi di colore verde chiaro, contrassegnati dalle rispettive icone e informazioni sullo stato. [Dettagli >>](#)
- **Collegamenti rapidi Scansione / Aggiornamento :** sono posizionati nella riga di pulsanti in basso nella finestra principale. Questi pulsanti consentono un accesso immediato alle funzionalità più importanti e più utilizzate di AVG. [Dettagli >>](#)

Oltre alla finestra principale di **AVG Internet Security** è presente un altro elemento di controllo che consente di accedere all'applicazione:

- **Icona dell'area di notifica:** posizionata nell'angolo inferiore destro dello schermo (*nell'area di notifica*), indica lo stato corrente di **AVG Internet Security**. [Dettagli >>](#)

### 3.3.1. Menu di spostamento superiore

Nel **menu di spostamento superiore** sono presenti diversi collegamenti attivi allineati nella parte superiore della finestra principale. Il menu di spostamento include i seguenti pulsanti:

#### 3.3.1.1. Altro da AVG

Fare clic sul collegamento per accedere al sito Web di AVG dove sono disponibili tutte le informazioni sulla protezione offerta da AVG per la massima sicurezza in Internet.

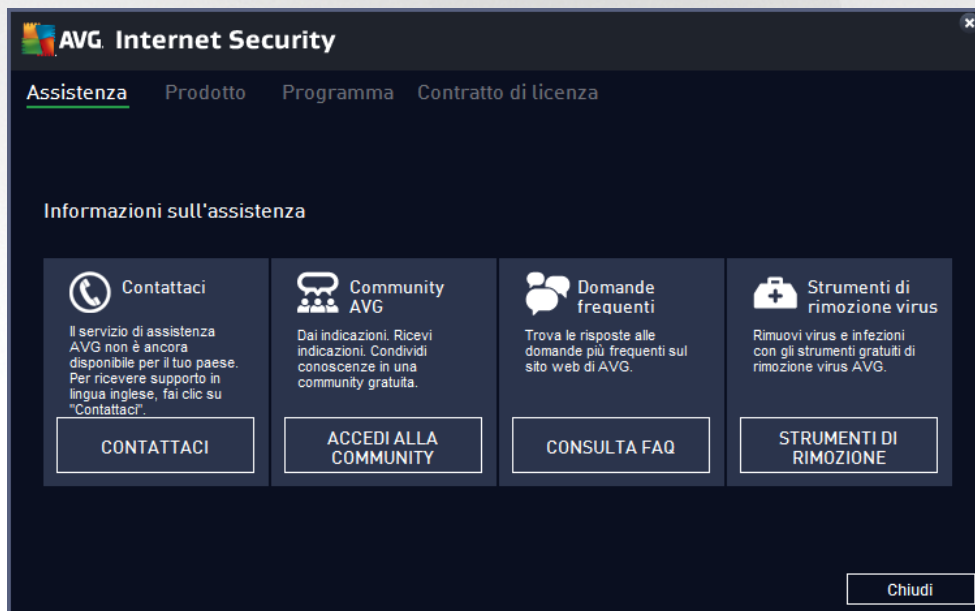
#### 3.3.1.2. Rapporti

Consente di aprire una nuova finestra di dialogo **Rapporti** con una panoramica di tutti i rapporti relativi alla scansioni avviate in precedenza e ai processi aggiornati. Se la scansione o l'aggiornamento è attualmente in esecuzione, verrà visualizzata un'icona rotante accanto al testo **Rapporti** nel menu di esplorazione superiore dell'[interfaccia utente principale](#). Fare clic su tale icona per visualizzare nella finestra di dialogo l'avanzamento del processo in esecuzione:



### 3.3.1.3. Assistenza

Aprire una nuova finestra di dialogo composta da quattro schede in cui è possibile trovare tutte le informazioni rilevanti su **AVG Internet Security**:



- **Assistenza** - questa scheda fornisce una panoramica organizzata in modo chiaro di tutti i contatti disponibili per l'assistenza clienti.
- **Prodotto** - questa scheda offre una panoramica dei dati tecnici più importanti di **AVG Internet Security**, quali informazioni sul prodotto antivirus, sui componenti installati e sulla protezione email installata.
- **Programma** - in questa scheda è possibile trovare informazioni tecniche dettagliate sul programma





**AVG Internet Security** installato, come il numero di versione del prodotto principale e l'elenco dei numeri di versione di tutti i prodotti corrispondenti (*ad esempio Zen, PC TuneUp, ...*). Questa scheda fornisce quindi una panoramica di tutti i componenti installati e informazioni specifiche sulla sicurezza (*numeri di versione di database dei virus, LinkScanner e Anti-Spam*).

- **Contratto di licenza** - in questa scheda è disponibile il testo completo del Contratto di licenza tra l'utente e AVG Technologies.

### **3.3.1.4. Opzioni**

La manutenzione di **AVG Internet Security** è accessibile tramite la voce **Opzioni**. Fare clic sulla freccia per aprire il menu a discesa:

- **Scansione computer** avvia una scansione dell'intero computer.
- **Scansione cartella selezionata...** - consente di passare all'interfaccia di scansione di AVG e di definire i file e le cartelle da sottoporre a scansione nella struttura del computer.
- **Scansione file...** - consente di eseguire un controllo su richiesta di un singolo file specifico. Fare clic su questa opzione per aprire una nuova finestra con la struttura del disco. Selezionare il file desiderato e confermare l'avvio della scansione.
- **Aggiorna** - avvia automaticamente il processo di aggiornamento di **AVG Internet Security**.
- **Aggiorna dalla directory...** - esegue il processo di aggiornamento dai file di aggiornamento che si trovano in una cartella specifica sul disco locale. Tuttavia, questa opzione è consigliabile solo in caso di emergenza, come in situazioni in cui non è disponibile la connessione a Internet (ad esempio, il computer è stato infettato e si è disconnesso da Internet, il computer è connesso a una rete senza accesso a Internet e così via). Nella finestra appena aperta selezionare la cartella in cui è stato precedentemente posizionato il file di aggiornamento e avviare il processo di aggiornamento.
- **Quarantena virus** - consente di aprire l'interfaccia della finestra di quarantena (Quarantena virus) in cui AVG sposta tutte le infezioni rilevate. All'interno della quarantena i file infetti vengono isolati e la protezione del computer è garantita. Allo stesso tempo, i file infetti vengono archiviati per una possibile riparazione futura.
- **Cronologia** - Offre ulteriori opzioni specifiche nel sottomenu:
  - **Risultati scansione** - Consente di aprire una finestra di dialogo con una panoramica dei risultati della scansione.
  - **Risultati di Resident Shield** - Consente di aprire una finestra di dialogo con una panoramica delle minacce rilevate da Resident Shield.
  - **Risultati di Analisi del software** - Consente di aprire una finestra di dialogo con una panoramica delle minacce rilevate dal componente Analisi del software.
  - **Risultati di Protezione email** - Consente di aprire una finestra di dialogo con una panoramica degli allegati email rilevati come pericolosi dal componente Protezione email.
  - **Risultati di Online Shield** - Consente di aprire una finestra di dialogo con una panoramica delle minacce rilevate da Online Shield.





- [Log cronologia eventi](#) - Consente di aprire l'interfaccia di Log cronologia con una panoramica di tutte le azioni di **AVG Internet Security** registrate.
- [Log Firewall](#) - Consente di aprire una finestra di dialogo con una panoramica dettagliata di tutte le azioni del Firewall.
- [Impostazioni avanzate...](#) - Consente di aprire la finestra di dialogo delle impostazioni AVG avanzate in cui è possibile modificare la configurazione di **AVG Internet Security**. In genere è consigliabile mantenere le impostazioni dell'applicazione predefinite dal fornitore del software.
- [Impostazioni del Firewall...](#) - Consente di aprire una finestra di dialogo autonoma per la configurazione avanzata del componente Firewall.
- **Sommario Guida** - Consente di aprire i file della Guida di AVG.
- **Ottieni assistenza** - Consente di aprire la [finestra di dialogo dell'assistenza](#), in cui sono disponibili tutti i contatti e le informazioni per l'assistenza.
- **Web AVG personale** - consente di aprire il sito Web di AVG (<http://www.avg.com/>).
- **Informazioni sui virus e le minacce** - Consente di aprire l'enciclopedia dei virus online sul sito Web di AVG (<http://www.avg.com/>) in cui è possibile trovare informazioni dettagliate sul virus identificato.
- **MyAccount** - consente di aprire la pagina relativa alla registrazione del **sito Web AVG MyAccount** (<http://www.avg.com/>). La creazione di un account AVG consente di gestire facilmente le licenze e i prodotti AVG registrati, scaricare nuovi prodotti, controllare lo stato degli ordini o amministrare i dati personali e le password. Immettere i dati di registrazione. Solo i clienti che registrano il prodotto AVG possono ricevere assistenza tecnica gratuita.
- **Informazioni su AVG** - Consente di aprire una nuova finestra di dialogo con quattro schede in cui sono presenti i dati sul tipo di licenza acquistata e le informazioni disponibili sull'assistenza, il prodotto e il programma, oltre al testo completo del Contratto di licenza. *In alternativa, è possibile accedere a questa finestra di dialogo utilizzando il collegamento [Assistenza](#) nella finestra principale.*

### 3.3.2. Informazioni sullo stato di protezione

La sezione **Impostazioni sullo stato di protezione** si trova nella parte superiore della **AVG Internet Security** finestra principale. All'interno di questa sezione sono contenute le informazioni sullo stato di protezione corrente di **AVG Internet Security**. Qui di seguito è disponibile una panoramica delle possibili icone, con il relativo significato:



- l'icona verde indica che **AVG Internet Security è completamente funzionante**. Il computer è totalmente protetto, aggiornato e tutti i componenti installati funzionano correttamente.



- l'icona gialla indica **la configurazione non corretta di uno o più componenti**. È consigliabile controllare le relative proprietà/impostazioni. Non sono presenti problemi gravi in **AVG Internet Security** e probabilmente è stato deciso di disattivare un componente per qualche ragione. La protezione è comunque attiva. Tuttavia, prestare attenzione alle impostazioni del componente in cui si sono verificati problemi. Il componente configurato in modo errato verrà visualizzato con una striscia arancione di avviso nell'[interfaccia utente principale](#).

L'icona gialla viene inoltre visualizzata se, per qualche motivo, l'utente ha deciso di ignorare lo stato di





errore di un componente. L'opzione **Ignora lo stato di errore** è accessibile nel ramo [Impostazioni avanzate / Ignora stato di errore](#). Qui è presente l'opzione per confermare che si è al corrente dello stato di errore del componente, tuttavia si desidera mantenere **AVG Internet Security** nella condizione attuale e non si desidera ricevere notifiche a riguardo. Potrebbe essere necessario utilizzare l'opzione **Ignora stato del componente** in situazioni particolari, tuttavia si consiglia di disattivare questa opzione nel più breve tempo possibile.

In alternativa, l'icona gialla verrà visualizzata anche se **AVG Internet Security** richiede il riavvio del computer (**Riavvio necessario**). Prestare attenzione all'avviso e riavviare il PC.



- l'icona arancione indica che **AVG Internet Security si trova in uno stato critico**. Uno o più componenti non funzionano correttamente e **AVG Internet Security** non è in grado di proteggere il computer. Intervenire immediatamente per risolvere il problema segnalato! Se non si è in grado di correggere l'errore, contattare il team dell'[Assistenza tecnica di AVG](#).

**Se AVG Internet Security non è impostato in modo da ottenere prestazioni ottimali, un nuovo pulsante denominato Risolvi problema (oppure Fare clic per risolvere i problemi, se sono interessati più componenti) appare accanto alle informazioni sullo stato di protezione. Selezionare il pulsante per avviare un processo automatico di controllo e configurazione del programma. Si tratta di un modo per impostare facilmente AVG Internet Security per ottenere prestazioni ottimali e massima protezione.**

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

**Nota:** le informazioni sullo stato di AVG Internet Security sono sempre disponibili anche tramite l'icona dell'area di notifica.

### 3.3.3. Panoramica dei componenti

La **panoramica dei componenti installati** è disponibile nella sezione centrale della [finestra principale](#). I componenti vengono visualizzati come blocchi di colore verde chiaro, contrassegnati dalle rispettive icone. Ogni blocco fornisce informazioni sullo stato corrente della protezione. Se il componente è stato configurato correttamente ed è completamente funzionante, l'informazione viene riportata in caratteri verdi. Se il componente viene arrestato e la relativa funzionalità viene limitata o se il componente si trova in stato di errore, l'utente verrà informato tramite un messaggio di avviso visualizzato in un campo di testo arancione. **Si consiglia di controllare le impostazioni del componente.**

Spostare il puntatore sul componente per visualizzare un breve testo nella parte inferiore della [finestra principale](#). Il testo fornisce un'introduzione di base alla funzionalità del componente. Comunica inoltre lo stato corrente del componente e specifica quali servizi del componente non sono configurati correttamente.

#### Elenco dei componenti installati

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

- **Computer** - questo componente comprende due servizi: **AntiVirus Shield**, che rileva virus, spyware, worm, trojan, librerie o file eseguibili indesiderati presenti nel sistema e protegge da adware dannoso, ed **Anti-Rootkit**, in grado di ricercare i rootkit pericolosi nascosti in applicazioni, driver o librerie. [Dettagli >>](#)





- **Esplorazione Web** - assicura la protezione dagli attacchi basati sul Web durante le ricerche e l'esplorazione online. [Dettagli >>](#)
- **Software** - questo componente esegue il servizio **Analisi del software**, che assicura la protezione costante delle risorse digitali contro le nuove minacce online. [Dettagli >>](#)
- **Email** - controlla la presenza di SPAM nei messaggi email in arrivo e blocca virus, attacchi di phishing o altre minacce. [Dettagli >>](#)
- **Firewall** - controlla tutte le comunicazioni in tutte le porte di rete, proteggendo il PC da attacchi pericolosi e bloccando tutti i tentativi di intrusione. [Dettagli >>](#)

#### Azioni accessibili

- **Posizionare il mouse sull'icona di un componente** per evidenziarlo all'interno della panoramica dei componenti. Nella parte inferiore dell'[interfaccia utente](#) viene inoltre visualizzata la descrizione delle funzionalità di base del componente.
- **Fare clic sull'icona del componente** per aprire l'interfaccia con le informazioni relative allo stato corrente e accedere alla configurazione e ai dati statistici del componente.

### 3.3.4. Collegamenti rapidi Scansione / Aggiornamento

**I collegamenti rapidi** sono disponibili nella riga di pulsanti in basso nell'[interfaccia utente](#) di **AVG Internet Security**. Questi collegamenti consentono di accedere immediatamente alle funzionalità più importanti e più utilizzate dell'applicazione, ovvero scansione e aggiornamento. I collegamenti rapidi sono accessibili da tutte le finestre di dialogo dell'interfaccia utente:

- **Esegui scansione** - questo pulsante è diviso graficamente in due sezioni. Selezionare il collegamento **Esegui scansione** per avviare la [Scansione intero computer](#) e visualizzare l'avanzamento e i relativi risultati nella finestra [Rapporti](#), che viene aperta automaticamente. Il pulsante **Opzioni** apre la finestra di dialogo **Opzioni di scansione** in cui è possibile [gestire le scansioni pianificate](#) e modificare i parametri di [Scansione intero computer](#) / [Scansione file o cartelle](#). *Per informazioni dettagliate, vedere il capitolo [Scansione AVG](#).*
- **Ottimizza le prestazioni** - questo pulsante consente di accedere al servizio [PC Analyzer](#), uno strumento avanzato per l'analisi e la correzione dettagliate del sistema che permette di migliorare la velocità e le prestazioni complessive del computer.
- **Aggiorna adesso**: premere questo pulsante per avviare subito l'aggiornamento del prodotto. I risultati dell'aggiornamento verranno visualizzati nella finestra a comparsa sopra l'icona di AVG nell'area di notifica. *Per informazioni dettagliate, vedere il capitolo [Aggiornamenti di AVG](#).*

### 3.3.5. AVG Advisor

**AVG Advisor** è stato progettato per rilevare i problemi che potrebbero mettere a rischio la protezione del computer e per suggerire una soluzione. **AVG Advisor** viene visualizzato in una finestra popup nell'area di notifica. Il servizio rileva la presenza di eventuali **reti sconosciute con nomi familiari**. Questa situazione in genere si applica solo agli utenti che si connettono a più reti, solitamente con computer portatili. Se una nuova rete sconosciuta ha lo stesso nome di una rete nota e utilizzata di frequente, *ad esempio Casa o Wi-Fi*, l'utente potrebbe collegarsi accidentalmente a una rete completamente sconosciuta e potenzialmente non sicura. **AVG Advisor** può impedire questa situazione segnalando che la rete apparentemente nota è in realtà una nuova rete. Se si decide che la nuova rete è sicura, è possibile salvarla nell'elenco delle reti note di **AVG**





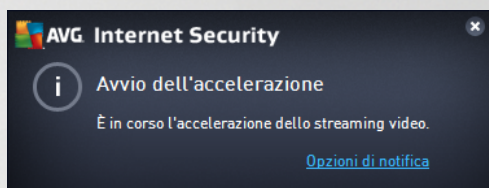
**Advisor**, in modo che non venga più segnalata in seguito.

### Browser Web supportati

La funzionalità è compatibile con i seguenti browser Web: Internet Explorer, Chrome, Firefox, Opera, Safari.

### 3.3.6. AVG Accelerator

**AVG Accelerator** ottimizza la riproduzione dei video online e semplifica il download. Quando il processo di accelerazione video è in corso, l'utente ne verrà informato tramite la finestra a comparsa nell'area di notifica.



## 3.4. Componenti di AVG

### 3.4.1. Protezione del computer


Il componente **Computer** comprende due servizi di protezione principali: **AntiVirus** e **Archivio dati protetto**.


- **AntiVirus** è costituito da un motore di scansione che controlla tutti i file, le aree di sistema del computer e i supporti rimovibili (*unità flash e così via*) e ricerca i virus noti. Tutti i virus rilevati vengono bloccati per essere poi corretti o messi in [Quarantena virus](#). Questo processo non viene notato dall'utente, poiché la protezione permanente viene eseguita "in background". AntiVirus utilizza anche la scansione euristica, che consente di rilevare le caratteristiche tipiche dei virus. In questo modo AntiVirus è in grado di rilevare un nuovo virus sconosciuto, se tale virus contiene alcune caratteristiche tipiche dei virus esistenti. **AVG Internet Security** è inoltre in grado di analizzare e rilevare le applicazioni eseguibili o le librerie DLL che potrebbero essere potenzialmente indesiderate nel sistema (*vari tipi di spyware, adware e così via*). Inoltre, AntiVirus esegue la scansione del Registro di sistema alla ricerca di voci sospette e file Internet temporanei e consente di trattare tutti gli elementi potenzialmente indesiderati come avviene per le altre infezioni.
- **Archivio dati protetto** consente di creare archivi virtuali protetti per archiviare dati sensibili o importanti. Il contenuto di un archivio dati protetto viene crittografato e protetto con una password definita dall'utente, in modo da renderlo inaccessibile a chi non dispone dall'autorizzazione.




### Comandi della finestra di dialogo

Per passare da una sezione all'altra della finestra di dialogo, è possibile fare clic in qualsiasi punto del pannello relativo al servizio desiderato. Il pannello viene evidenziato in una tonalità di blu più chiara. In entrambe le sezioni della finestra di dialogo sono disponibili i seguenti controlli. Il funzionamento è identico, indipendentemente dal servizio di protezione a cui appartengono (*AntiVirus* o *Archivio dati protetto*):

 **Attivato / Disattivato** - questo pulsante è simile a un semaforo, sia nell'aspetto che nella funzionalità. Fare clic per passare da una posizione all'altra. Il colore verde rappresenta lo stato **Attivato**, ovvero indica che il servizio di protezione AntiVirus è attivo e completamente funzionante. Il colore rosso rappresenta lo stato **Disattivato**, ovvero indica che il servizio è disabilitato. A meno che non sussista un motivo valido per disattivare il servizio, si consiglia di mantenere le impostazioni predefinite per tutte le configurazioni di protezione. Le impostazioni predefinite assicurano prestazioni ottimali dell'applicazione e massima protezione. Se è necessario disattivare il servizio, per mettere in guardia dai possibili rischi viene visualizzato il segnale rosso di **Avviso** con la notifica che la protezione non è completa. **Tenere presente che è necessario riattivare il servizio il prima possibile.**

 **Impostazioni** - facendo clic su questo pulsante si viene reindirizzati all'area delle [impostazioni avanzate](#). Verrà aperta la relativa finestra di dialogo e sarà possibile configurare il servizio selezionato, ovvero [AntiVirus](#). Nell'area delle impostazioni avanzate è possibile modificare la configurazione di ogni servizio di protezione incluso in **AVG Internet Security**, tuttavia si sconsiglia agli utenti meno esperti di apportare modifiche.

 **Freccia** - usare la freccia verde nella parte superiore sinistra della finestra di dialogo per tornare alla panoramica dei componenti nell'[interfaccia utente principale](#).

### Come creare un archivio dati protetto

Nella sezione **Archivio dati protetto** della finestra di dialogo **Protezione del computer** è disponibile il pulsante **Crea archivio protetto**. Fare clic sul pulsante per aprire una nuova finestra di dialogo con lo stesso nome in cui è possibile specificare i parametri dell'archivio protetto da creare. Immettere le informazioni necessarie e seguire le istruzioni nell'applicazione:

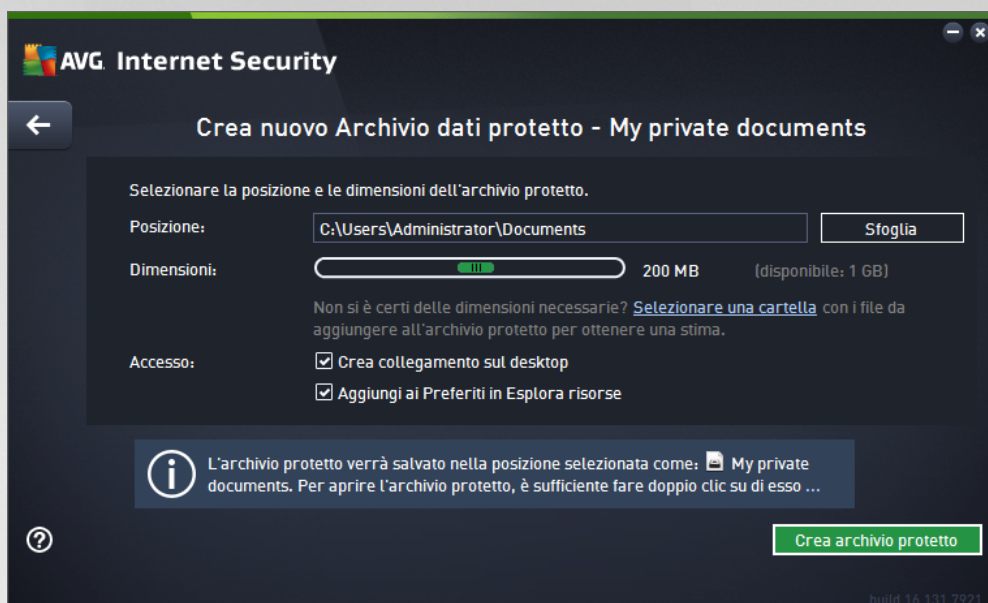




Innanzitutto è necessario specificare il nome dell'archivio protetto e creare una password complessa:

- **Nome archivio dati protetto** - per creare un nuovo archivio protetto, è innanzitutto necessario scegliere un nome appropriato per riconoscerlo. Se si condivide il computer con altri familiari, è consigliabile includere il proprio nome oltre all'indicazione del contenuto dell'archivio, ad esempio *Email di papà*.
- **Creare la password / Ridigitare la password** - creare una password per l'archivio dati protetto e digitarla nei rispettivi campi di testo. L'indicatore grafico a destra segnala se la password dell'utente è vulnerabile (*relativamente facile da identificare con speciali strumenti software*) o complessa. È consigliabile scegliere una password di complessità almeno media. È possibile rendere più sicura la password aggiungendo lettere maiuscole, numeri e altri caratteri come punti, trattini e così via. Per essere certi che la password sia stata digitata nel modo desiderato, è possibile selezionare la casella **Mostra password** (*ovviamente è necessario assicurarsi che nessuno stia guardando lo schermo*).
- **Suggerimento password** - è consigliabile creare anche un suggerimento utile per ricordare la password in caso di necessità. Tenere presente che un archivio dati protetto viene creato per proteggere i file consentendo l'accesso solo con la password. Non è possibile eludere la protezione e se si dimentica la password non sarà possibile accedere all'archivio dati protetto.

Dopo aver specificato nei campi di testo tutti i dati richiesti, fare clic sul pulsante **Avanti** per procedere al passaggio successivo:

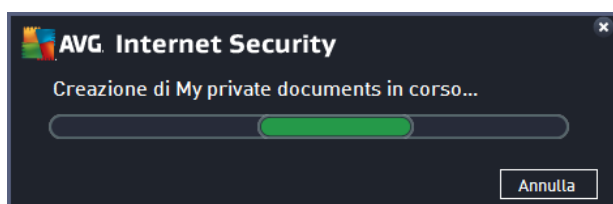


Questa finestra di dialogo fornisce le seguenti opzioni di configurazione:

- **Posizione:** indica dove verrà collocato fisicamente l'archivio protetto. Individuare una destinazione appropriata nel disco rigido oppure mantenere la posizione predefinita, ovvero la cartella *Documenti*. Tenere presente che dopo aver creato un archivio dati protetto non è possibile modificarne la posizione.
- **Dimensioni** - è possibile impostare le dimensioni predefinite dell'archivio dati protetto, in modo da allocare lo spazio necessario su disco. Il valore impostato non deve essere troppo piccolo (*insufficiente per le esigenze dell'utente*), né troppo grande (*tale da occupare troppo spazio su disco inutilmente*). Se è già stato deciso cosa trasferire nell'archivio dati protetto, è possibile inserire tutti i file in una cartella e utilizzare il collegamento **Selezionare una cartella** per calcolare automaticamente le dimensioni totali. È comunque possibile modificare le dimensioni in un secondo momento in base alle esigenze.
- **Accesso** - le caselle di controllo presenti in questa sezione consentono di creare collegamenti rapidi all'archivio dati protetto.

### Come utilizzare l'archivio dati protetto

Dopo aver configurato le impostazioni desiderate, fare clic sul pulsante **Crea archivio protetto**. Verrà visualizzata una nuova finestra di dialogo **L'archivio dati è pronto** che indica che l'archivio dati è pronto per l'archiviazione dei file. L'archivio dati è ora aperto ed è possibile accedervi immediatamente. In seguito, per accedere nuovamente all'archivio dati sarà necessario sbloccarlo con la password definita:



Per utilizzare il nuovo archivio dati protetto, è necessario innanzitutto aprirlo facendo clic sul pulsante **Apri**

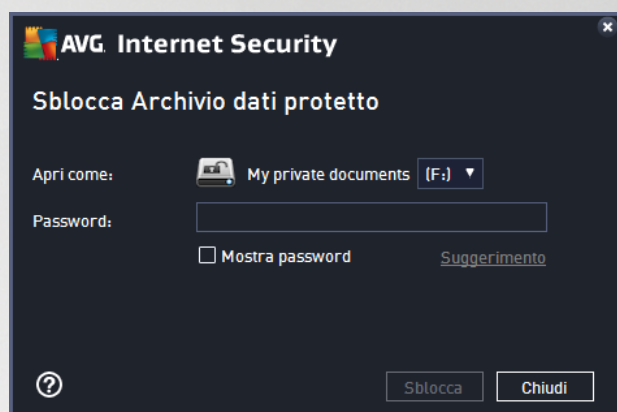




**subito.** Una volta aperto, l'archivio dati protetto verrà visualizzato nel computer come un nuovo disco virtuale. Assegnare all'archivio una lettera dal menu a discesa (è possibile selezionare solo i dischi attualmente liberi). In genere, non è consentito scegliere le lettere C (assegnata solitamente al disco rigido), A (unità disco floppy) o D (unità DVD). Tenere presente che ogni volta che si sblocca un archivio dati protetto è possibile scegliere una lettera diversa per l'unità tra quelle disponibili.

### Come sbloccare l'archivio dati protetto

Quando si tenta di accedere nuovamente all'archivio dati protetto viene richiesto di sbloccarlo utilizzando la password definita:



Digitare nel campo di testo la password di autorizzazione e fare clic sul pulsante **Sblocca**. Se non si riesce a ricordare la password, fare clic su **Suggerimento** per visualizzare il suggerimento per la password definito al momento della creazione dell'archivio dati protetto. Il nuovo archivio dati protetto verrà visualizzato nella panoramica degli archivi dati protetti come SBLOCCATO e sarà possibile aggiungere o rimuovere i file al suo interno in base alle esigenze.

### 3.4.2. Protezione esplorazione Web

La **Protezione esplorazione Web** è composta da due servizi: **LinkScanner Surf-Shield** e **Online Shield**:

- **LinkScanner Surf-Shield** protegge dal numero sempre crescente di minacce transitorie presenti sul Web. Queste minacce possono nascondersi in qualsiasi tipo di sito Web, da quelli degli enti governativi, a quelli di grandi marchi famosi, a quelli di piccole aziende, e raramente restano in questi siti per più di 24 ore. LinkScanner protegge gli utenti analizzando le pagine Web a cui puntano tutti i collegamenti presenti nella pagina Web visualizzata e garantendo che le pagine siano sicure nel momento cruciale, ovvero nell'attimo in cui si sta per fare clic sul collegamento. **Il componente LinkScanner Surf-Shield non è destinato alla protezione delle piattaforme server.**
- **Online Shield** è un tipo di protezione permanente in tempo reale che esegue la scansione del contenuto delle pagine Web visitate (e dei possibili file in esse contenuti) persino prima che vengano visualizzate nel browser Web o scaricate nel computer. Online Shield rileva se la pagina che sta per essere aperta contiene javascript dannosi e ne impedisce la visualizzazione. Inoltre, riconosce il malware contenuto in una pagina arrestandone immediatamente il download per impedirne il trasferimento nel computer. Si tratta di un potente strumento di protezione che blocca il contenuto pericoloso delle pagine Web quando si tenta di aprirle, impedendone il download sul computer. Se questa funzionalità è abilitata, quando si fa clic sul collegamento o si digita l'URL di un sito pericoloso, l'apertura della pagina Web verrà bloccata immediatamente impedendo che il PC dell'utente venga infettato. È importante tenere presente che le pagine Web dannose possono





infettare il computer con il semplice accesso al sito infetto. **Il componente Online Shield non è destinato alle piattaforme server.**




### Comandi della finestra di dialogo

Per passare da una sezione all'altra della finestra di dialogo, è possibile fare clic in qualsiasi punto del pannello relativo al servizio desiderato. Il pannello viene evidenziato in una tonalità di blu più chiara. In entrambe le sezioni della finestra di dialogo sono disponibili i seguenti controlli. La funzionalità è la stessa, indipendentemente dal servizio di protezione a cui appartengono (*LinkScanner Surf-Shield* o *Online Shield*):

 **Attivato / Disattivato** - questo pulsante è simile a un semaforo, sia nell'aspetto che nella funzionalità. Fare clic per passare da una posizione all'altra. Il colore verde significa **Attivato**, ovvero indica che il servizio di protezione LinkScanner Surf-Shield / Online Shield è attivo e completamente funzionante. Il colore rosso rappresenta lo stato **Disattivato**, ovvero indica che il servizio è disabilitato. A meno che non sussista un motivo valido per disattivare il servizio, si consiglia di mantenere le impostazioni predefinite per tutte le configurazioni di protezione. Le impostazioni predefinite assicurano prestazioni ottimali dell'applicazione e massima protezione. Se è necessario disattivare il servizio, per mettere in guardia dai possibili rischi viene visualizzato il segnale rosso di **Avviso** con la notifica che la protezione non è completa. **Tenere presente che è necessario riattivare il servizio il prima possibile.**

 **Impostazioni** - facendo clic su questo pulsante si viene reindirizzati all'area delle [impostazioni avanzate](#). Più precisamente, verrà aperta la rispettiva finestra di dialogo e l'utente potrà configurare il servizio selezionato, ovvero [LinkScanner Surf-Shield](#) o [Online Shield](#). Nell'area delle impostazioni avanzate è possibile modificare la configurazione di ogni servizio di protezione incluso in **AVG Internet Security**, tuttavia si sconsiglia agli utenti meno esperti di apportare modifiche.

 **Freccia** - usare la freccia verde nella parte superiore sinistra della finestra di dialogo per tornare alla panoramica dei componenti nell'[interfaccia utente principale](#).





### 3.4.3. Analisi del software

Il componente **Analisi del software** assicura la protezione costante delle risorse digitali contro le nuove minacce online:

- **Analisi del software** è un servizio anti-malware che protegge da tutti i tipi di malware (*spyware, bot, furto di identità e così via*) utilizzando tecnologie basate sul comportamento e fornisce la protezione zero day per i nuovi virus. Identity Protection è destinato alla prevenzione di attacchi da parte di malintenzionati volti a sottrarre password, dati dei conti bancari, numeri delle carte di credito e altri importanti dati digitali tramite qualsiasi tipo di software dannoso (*malware*) in grado di colpire il PC. L'applicazione assicura che tutti i programmi in esecuzione nel PC o nella rete condivisa funzionino correttamente. Analisi del software rileva e blocca i comportamenti sospetti in modo continuo e protegge il computer da tutti i nuovi malware. Analisi del software fornisce al computer protezione in tempo reale da minacce nuove e sconosciute. Monitora tutti i processi (*compresi quelli nascosti*) e oltre 285 diversi schemi di comportamento ed è in grado di determinare se nel sistema si stanno verificando operazioni dannose. Per tale motivo, può rilevare minacce non ancora descritte nel database dei virus. Quando un codice sconosciuto entra nel computer viene immediatamente controllato, per verificarne l'eventuale comportamento dannoso, e tracciato. Se si determina che il file è dannoso, Analisi del software rimuoverà il codice spostandolo in [Quarantena virus](#) e annulla le modifiche apportate al sistema (*iniezioni di codice, modifiche del registro, apertura di porte e così via*). Non è necessario avviare una scansione per essere protetti. La tecnologia è proattiva, richiede raramente l'aggiornamento ed è sempre attiva.



#### Comandi della finestra di dialogo


Nella finestra di dialogo sono disponibili i seguenti controlli:


- **Attivato / Disattivato** - questo pulsante è simile a un semaforo, sia nell'aspetto che nella funzionalità. Fare clic per passare da una posizione all'altra. Il verde rappresenta lo stato **Attivato**, ovvero indica che il servizio di protezione Analisi del software è attivo e completamente funzionante. Il colore rosso rappresenta lo stato **Disattivato**, ovvero indica che il servizio è disabilitato. A meno che non sussista un motivo valido per disattivare il servizio, si consiglia di mantenere le impostazioni predefinite per tutte le configurazioni di protezione. Le impostazioni predefinite assicurano prestazioni ottimali





dell'applicazione e massima protezione. Se è necessario disattivare il servizio, per mettere in guardia dai possibili rischi viene visualizzato il segnale rosso di **Avviso** con la notifica che la protezione non è completa. **Tenere presente che è necessario riattivare il servizio il prima possibile.**

 **Impostazioni** - facendo clic su questo pulsante si accede all'area delle [impostazioni avanzate](#). Nella finestra di dialogo visualizzata è possibile configurare il servizio selezionato, ovvero [Analisi del software](#). Nell'area delle impostazioni avanzate è possibile modificare la configurazione di tutti i servizi di protezione inclusi in **AVG Internet Security**, tuttavia si sconsiglia agli utenti meno esperti di apportare modifiche.

 **Freccia** - usare la freccia verde nella parte superiore sinistra della finestra di dialogo per tornare alla panoramica dei componenti nell'[interfaccia utente principale](#).

Purtroppo in **AVG Internet Security** il servizio Identity Alert non è incluso. Se si desidera utilizzare questo tipo di protezione, fare clic sul pulsante **Aggiorna per attivare** per essere reindirizzati alla pagina Web dedicata in cui è possibile acquistare la licenza di Identity Alert.

*Tenere presente che anche nelle edizioni AVG Premium Security, il servizio Identity Alert è attualmente disponibile solo nei seguenti paesi: Stati Uniti, Regno Unito, Canada e Irlanda.*

### 3.4.4. Protezione email

Il componente **Protezione email** include i due seguenti servizi di protezione: **Scansione Email** e **Anti-Spam** (il servizio Anti-Spam è accessibile solo nelle edizioni Internet/Premium Security).


- **Scansione Email:** Una delle origini più comuni di virus e trojan è l'email. Phishing e spam rendono l'email una fonte di rischio ancora più grande. Gli account email gratuiti sono quelli che presentano più probabilità di ricevere questo tipo di messaggi dannosi, *poiché raramente impiegano una tecnologia antispam*, e gli utenti domestici si affidano moltissimo a questo tipo di email. Inoltre, gli utenti domestici aumentano l'esposizione ad attacchi tramite email poiché navigano spesso in siti sconosciuti e compilano moduli online con dati personali, *ad esempio l'indirizzo email*. Di solito le società utilizzano account aziendali, filtri antispam e altri accorgimenti per ridurre il rischio. Il componente Protezione email è responsabile della scansione di tutti i messaggi email inviati o ricevuti. Ogni volta che viene rilevato un virus in un'email, questo viene immediatamente spostato in [Quarantena virus](#). Il componente, inoltre, può filtrare alcuni tipi di allegati email e aggiungere un testo di certificazione ai messaggi non infetti. **Il componente Scansione Email non è destinato alle piattaforme server.**
- **Anti-Spam** consente di controllare tutti i messaggi email in arrivo e di contrassegnare quelli indesiderati come spam (*il termine "spam" indica messaggi di posta indesiderati, per lo più pubblicità di prodotti o servizi, inviate in massa e simultaneamente a un enorme numero di indirizzi di posta elettronica, che intasano le cassette postali dei destinatari. Lo spam non rientra nella categoria dei legittimi messaggi email commerciali per i quali i consumatori hanno fornito il consenso.*). Anti-Spam può modificare l'oggetto dell'email (*identificata come spam*) aggiungendo una stringa di testo speciale. Sarà quindi possibile filtrare rapidamente i messaggi email nel client email. Il componente Anti-Spam utilizza diversi metodi di analisi per elaborare ciascun messaggio email, offrendo il massimo livello di protezione possibile contro i messaggi email indesiderati. Anti-Spam utilizza un database aggiornato regolarmente per il rilevamento dello spam. È inoltre possibile utilizzare i [server RBL](#) (*database pubblici di indirizzi email di "spammer noti"*) e aggiungere manualmente indirizzi email alla [whitelist](#) (*indirizzi da non contrassegnare mai come spam*) e alla [blacklist](#) (*indirizzi da contrassegnare sempre come spam*).







### Comandi della finestra di dialogo

Per passare da una sezione all'altra della finestra di dialogo, è possibile fare clic in qualsiasi punto del pannello relativo al servizio desiderato. Il pannello viene evidenziato in una tonalità di blu più chiara. In entrambe le sezioni della finestra di dialogo sono disponibili i seguenti controlli. La funzionalità è la stessa, indipendentemente dal servizio di protezione a cui appartengono (*Scansione Email* o *Anti-Spam*):

 **Attivato / Disattivato** - questo pulsante è simile a un semaforo, sia nell'aspetto che nella funzionalità. Fare clic per passare da una posizione all'altra. Il colore verde significa **Attivato**, ovvero indica che il servizio di protezione è attivo e completamente funzionante. Il colore rosso rappresenta lo stato **Disattivato**, ovvero indica che il servizio è disabilitato. A meno che non sussista un motivo valido per disattivare il servizio, si consiglia di mantenere le impostazioni predefinite per tutte le configurazioni di protezione. Le impostazioni predefinite assicurano prestazioni ottimali dell'applicazione e massima protezione. Se è necessario disattivare il servizio, per mettere in guardia dai possibili rischi viene visualizzato il segnale rosso di **Avviso** con la notifica che la protezione non è completa. **Tenere presente che è necessario riattivare il servizio il prima possibile.**

 **Impostazioni** - facendo clic su questo pulsante si viene reindirizzati all'area delle [impostazioni avanzate](#). Verrà aperta la relativa finestra di dialogo e sarà possibile configurare il servizio selezionato, ovvero [Scansione Email](#) o [Anti-Spam](#). Nell'area delle impostazioni avanzate è possibile modificare la configurazione di ogni servizio di protezione incluso in **AVG Internet Security**, tuttavia si sconsiglia agli utenti meno esperti di apportare modifiche.

 **Freccia** - usare la freccia verde nella parte superiore sinistra della finestra di dialogo per tornare alla panoramica dei componenti nell'[interfaccia utente principale](#).

### 3.4.5. Firewall

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



accedere al PC. Il componente Firewall viene configurato per consentire o negare le comunicazioni interne/esterne (in entrambe le direzioni, entrata o uscita) tramite le porte definite e per le applicazioni software definite. Ad esempio, potrebbe essere configurato per consentire il solo flusso dei dati Web in entrata e in uscita tramite Microsoft Internet Explorer. Qualsiasi tentativo di trasmettere i dati Web tramite un altro browser viene quindi bloccato. Il componente Firewall impedisce l'invio non autorizzato delle informazioni di identificazione personale contenute nel computer. Controlla il modo in cui il computer scambia dati con altri computer in Internet o nella rete locale. All'interno di un'organizzazione il componente Firewall protegge anche i singoli computer da attacchi lanciati da utenti interni ai computer nella rete.

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

**AVG Firewall non è destinato alla protezione delle piattaforme server.**

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



**Nota:** dopo l'installazione di AVG Internet Security, il componente Firewall potrebbe richiedere il riavvio del computer. In tal caso, verrà visualizzata la finestra di dialogo del componente che comunica che è necessario riavviare il computer. Il pulsante **Riavvia ora** è disponibile direttamente nella finestra di dialogo. Fino al riavvio, il componente Firewall non è completamente attivato e anche le relative opzioni di modifica all'interno della finestra di dialogo sono disabilitate. Prestare attenzione all'avviso e riavviare il PC appena possibile.

### Modalità Firewall disponibili

Il componente Firewall consente di definire le regole di protezione specifiche a seconda che si tratti di un





computer presente in un dominio, di un computer autonomo o perfino di un notebook. Ogni opzione richiede un livello diverso di protezione e i livelli sono coperti dalle rispettive modalità. In breve, una modalità Firewall è una specifica configurazione del componente Firewall ed è possibile utilizzare diverse di queste configurazioni predefinite.

- **Automatica** - in questa modalità il componente Firewall gestisce tutto il traffico di rete automaticamente. Non verrà richiesto l'intervento dell'utente. Il componente Firewall consentirà la connessione a tutte le applicazioni note e contemporaneamente verrà creata una regola che indica che tale applicazione può connettersi sempre in futuro. Per altre applicazioni, Firewall deciderà se consentire o bloccare la connessione in base al comportamento dell'applicazione. Tuttavia, in questa situazione non verrà creata alcuna regola e l'applicazione verrà controllata nuovamente quando tenta di connettersi. La modalità automatica è abbastanza discreta ed è consigliata per la maggior parte degli utenti.
- **Interattiva** - questa modalità è utile se si desidera controllare completamente tutto il traffico di rete in ingresso e in uscita dal computer. Il componente Firewall monitorerà il traffico e notificherà all'utente ogni tentativo di comunicazione o trasferimento dati, permettendo all'utente di consentire o bloccare i tentativi come desidera. Opzione consigliata solo per utenti esperti.
- **Blocca l'accesso a Internet** - la connessione a Internet viene bloccata completamente, è impossibile accedere a Internet e nessuno può accedere al computer dall'esterno. Solo per uso eccezionale e per breve tempo.
- **Disattiva la protezione Firewall (opzione non consigliata)** - la disattivazione del Firewall consentirà tutto il traffico di rete in entrata e in uscita dal computer. Di conseguenza, il computer sarà esposto agli attacchi di hacker. Valutare sempre questa opzione con attenzione.

Tenere presente che una modalità automatica specifica è disponibile anche nel Firewall. Questa modalità viene attivata in modo invisibile se i componenti [Protezione del computer](#) o [Analisi del software](#) vengono disattivati rendendo il computer più vulnerabile. In tali casi, il componente Firewall consentirà automaticamente solo le applicazioni note e assolutamente sicure. Per tutti gli altri casi, verrà richiesto all'utente come procedere. Ciò consente di oviare alla disattivazione dei componenti di protezione e di mantenere il computer protetto.

***Si consiglia di non disattivare mai il Firewall. Tuttavia, se ci fosse necessità di disattivare il componente Firewall, è possibile farlo selezionando la modalità Disattiva la protezione Firewall dall'elenco delle modalità Firewall disponibili.***

### Comandi della finestra di dialogo

La finestra di dialogo fornisce una panoramica delle informazioni di base sullo stato del componente Firewall:


- **Modalità Firewall** - fornisce informazioni sulla modalità Firewall attualmente selezionata. Utilizzare il pulsante **Modifica** accanto all'informazione fornita per passare all'interfaccia [Impostazioni del Firewall](#) se si desidera modificare la modalità corrente con un'altra (*per descrizioni e consigli sull'utilizzo dei profili Firewall vedere il paragrafo precedente*).
- **Condivisione file e stampanti** - indica se la condivisione di file e stampanti (*in entrambe le direzioni*) al momento è disponibile. Condivisione di file e stampanti significa condividere qualsiasi file o cartella contrassegnato come "Condiviso" in Windows, in unità disco comuni, stampanti, scanner e dispositivi simili. È preferibile condividere tali elementi solo all'interno di reti considerate sicure (*ad esempio a casa, in ufficio o a scuola*). Tuttavia, se si è connessi a una rete pubblica (*ad esempio, al Wi-Fi dell'aeroporto o di un Internet Point*), è consigliabile non condividere nulla.






- **Connesso a** - fornisce informazioni sul nome della rete a cui si è attualmente connessi. Con Windows XP, il nome della rete corrisponde alla denominazione scelta per la rete specifica durante la prima connessione. Con Windows Vista e versioni successive, il nome della rete viene ricavato automaticamente dal Centro connessioni di rete e condivisione.
- **Reimposta su predefinito** - selezionare questo pulsante per sovrascrivere la configurazione corrente del Firewall e ripristinare la configurazione predefinita basata sul rilevamento automatico.

Nella finestra di dialogo sono disponibili i seguenti comandi grafici:

 **Impostazioni** - fare clic sul pulsante per aprire un menu in cui sono disponibili due opzioni:

- **Impostazioni avanzate** - questa opzione reindirizza all'interfaccia [Impostazioni del firewall](#), in cui è possibile modificare tutta la configurazione del componente Firewall. Tenere tuttavia presente che qualunque configurazione deve essere eseguita solo da utenti esperti.
- **Rimuovi protezione Firewall** - questa opzione consente di disinstallare il componente Firewall, benché tale operazione possa ridurre il livello di protezione. Se si desidera comunque rimuovere il componente Firewall, confermare la decisione e il componente verrà disinstallato completamente.



 **Freccia** - usare la freccia verde nella parte superiore sinistra della finestra di dialogo per tornare alla panoramica dei componenti nell'[interfaccia utente principale](#).

### 3.4.6. PC Analyzer

Il componente **PC Analyzer** è uno strumento avanzato per l'analisi e la correzione dettagliate del sistema che consente di migliorare la velocità e le prestazioni complessive del computer. Si apre attraverso l'opzione **Ottimizza le prestazioni** disponibile nella [finestra di dialogo dell'interfaccia utente principale](#) o tramite la stessa opzione disponibile nel menu di scelta rapida dell'icona di AVG dell'area di notifica. Sarà quindi possibile visualizzare l'avanzamento dell'analisi e i relativi risultati direttamente nel grafico:



The screenshot shows the AVG Internet Security PC Analyzer window. At the top, it says 'AVG Internet Security' and 'PC Analyzer'. Below that, a green checkmark indicates 'PC Analyzer ha terminato l'analisi'. The main area is a table with three columns: 'Categoria', 'Risultati', and 'Gravità'. There are four rows of data, each with an icon, a category name, a description, the number of errors found, a 'Dettagli...' link, and a progress bar. At the bottom, there is a green button labeled 'Correggi ora' and a small text box about downloading 'AVG PC TuneUp'.

Categoria	Risultati	Gravità
 <b>Errori di registro</b> Influiscono sulla stabilità del sistema	106 errori trovati <a href="#">Dettagli...</a>	
 <b>File inutili</b> Occupano spazio su disco	495 errori trovati <a href="#">Dettagli...</a>	
 <b>Frammentazione</b> Riduce la velocità di accesso al disco	17% frammentato <a href="#">Dettagli...</a>	
 <b>Collegamenti interrotti</b> Riducono la velocità di esplorazione	29 errori trovati <a href="#">Dettagli...</a>	

Scarica il nuovo componente [AVG PC TuneUp](#) per effettuare una correzione degli errori gratuitamente, o acquista una licenza per avere diritto a 12 mesi di correzioni illimitate. [Correggi ora](#)

build 7132

È possibile analizzare le seguenti categorie: errori di registro, file inutili, frammentazione e collegamenti





interrotti:

- **Errori di registro** fornisce il numero di errori presenti nel Registro di Windows che potrebbero causare rallentamenti del computer o la visualizzazione di messaggi di errore.
- **File inutili** fornisce il numero di file che consumano spazio su disco e che molto probabilmente sono superflui. In genere si tratta di file temporanei di vario tipo e dei file presenti nel Cestino.
- **Frammentazione** consente di calcolare la percentuale di disco rigido frammentata, ovvero utilizzata per molto tempo per cui al momento numerosi file si trovano sparsi in diverse parti del disco fisico.
- **Collegamenti interrotti** individua collegamenti non più funzionanti, che conducono a posizioni inesistenti e così via.

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

#### **Pulsanti di controllo**

- **Arresta analisi** (*visualizzato durante l'esecuzione dell'analisi*): selezionare questo pulsante per interrompere l'analisi del computer.
- **Installare per correggere** (*visualizzato al termine dell'analisi*): la funzionalità di PC Analyzer in **AVG Internet Security** è limitata all'analisi dello stato presente del PC. Tuttavia, AVG fornisce uno strumento avanzato per l'analisi e la correzione dettagliate del sistema che consente di migliorare la velocità e le prestazioni complessive del computer. Fare clic sul pulsante per essere reindirizzati alla pagina Web dedicata in cui sono disponibili ulteriori informazioni.

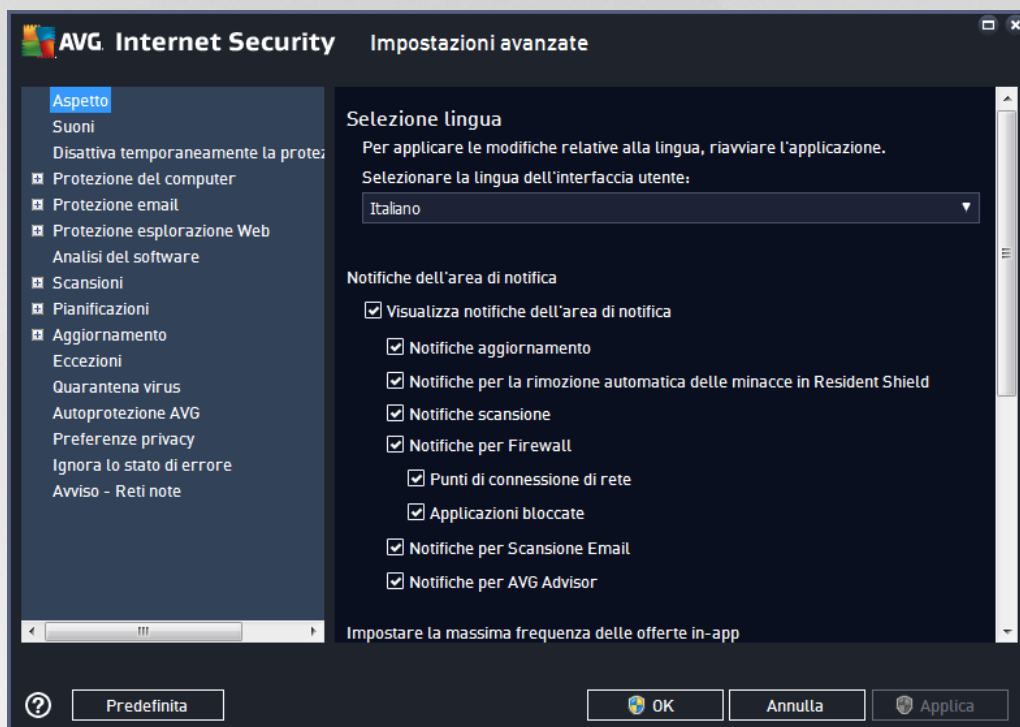
### **3.5. Impostazioni avanzate di AVG**

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



### 3.5.1. Aspetto

La prima voce della struttura di esplorazione, **Aspetto**, fa riferimento alle impostazioni generali dell'[interfaccia utente](#) di **AVG Internet Security** e fornisce alcune opzioni di base relative al comportamento dell'applicazione:

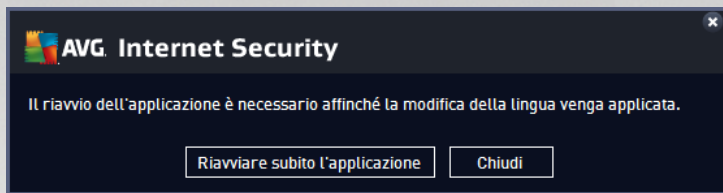


#### Selezione lingua

Nella sezione **Selezione lingua** è possibile scegliere la lingua desiderata dal menu a discesa. La lingua selezionata verrà utilizzata per l'intera [interfaccia utente](#) di **AVG Internet Security**. Nel menu a discesa sono presenti solo le lingue selezionate in precedenza per essere installate durante il processo di installazione e l'inglese (*sempre installato automaticamente per impostazione predefinita*). Per completare l'impostazione di **AVG Internet Security** su un'altra lingua è necessario riavviare l'applicazione. Procedere come segue:

- Nel menu a discesa, selezionare la lingua desiderata per l'applicazione
- Confermare la selezione facendo clic sul pulsante **Applica** nell'angolo inferiore destro della finestra di dialogo
- Fare clic sul pulsante **OK** per confermare
- Viene visualizzata una nuova finestra di dialogo che comunica che per modificare la lingua dell'applicazione è necessario riavviare **AVG Internet Security**
- Fare clic sul pulsante **Riavvia subito AVG** per confermare il riavvio del programma e attendere alcuni istanti l'applicazione della modifica della lingua:





## Notifiche dell'area di notifica

In questa sezione è possibile disattivare la visualizzazione delle notifiche dell'area di notifica sullo stato dell'applicazione **AVG Internet Security**. Per impostazione predefinita, le notifiche della barra delle applicazioni vengono visualizzate. Si consiglia di mantenere questa impostazione. Le notifiche di sistema comunicano, ad esempio, l'avvio del processo di scansione o aggiornamento o una modifica dello stato di un componente di **AVG Internet Security**. Questi avvisi devono essere tenuti nella dovuta considerazione.

Tuttavia, se non si desidera visualizzare tali notifiche o si desidera visualizzarne solo alcune (*correlate a un particolare componente di AVG Internet Security*), è possibile specificare le proprie preferenze selezionando/deselezionando le seguenti opzioni:

- **Visualizza notifiche dell'area di notifica** (*attivata per impostazione predefinita*) - per impostazione predefinita, tutte le notifiche vengono visualizzate. Deselezionare questa voce per disattivare completamente la visualizzazione delle notifiche di sistema. Quando è attivata, è possibile selezionare inoltre le notifiche specifiche da visualizzare:
  - **Notifiche aggiornamento** (*attivata per impostazione predefinita*) - consente di decidere se visualizzare le informazioni relative **AVG Internet Security** all'avvio, all'avanzamento e alla finalizzazione del processo di aggiornamento.
  - **Notifiche per la rimozione automatica delle minacce in Resident Shield** (*attivata per impostazione predefinita*) - consente di decidere se visualizzare o meno le informazioni relative ai processi di salvataggio, copia e apertura dei file (*questa configurazione viene visualizzata solo se l'opzione Correzione automatica di Resident Shield è attiva*).
  - **Notifiche scansione** (*attivata per impostazione predefinita*) - consente di decidere se visualizzare le informazioni relative all'avvio automatico, all'avanzamento e ai risultati della scansione pianificata.
  - **Notifiche Firewall** (*attivata per impostazione predefinita*) - consente di decidere se visualizzare le informazioni relative ai processi e allo stato del componente Firewall, quali avvisi di attivazione/disattivazione del componente, possibile blocco del traffico. Questa voce fornisce altre due opzioni di selezione specifiche (*per informazioni dettagliate su queste opzioni, vedere il capitolo [Firewall](#) di questo documento*):
    - **Punti di connessione di rete** (*disattivata per impostazione predefinita*): durante la connessione a una rete, indica se la rete è nota e come verrà impostata la condivisione di file e stampanti.
    - **Applicazioni bloccate** (*attivata per impostazione predefinita*): quando un'applicazione sconosciuta o sospetta tenta di connettersi a una rete, blocca il tentativo e visualizza una notifica. Questa funzionalità è utile per tenere informato l'utente, pertanto è consigliabile mantenerla sempre attivata.
  - **Notifiche per Scansione Email** (*attivata per impostazione predefinita*) - consente di decidere



se visualizzare le informazioni relative alla scansione di tutti i messaggi email in entrata e in uscita.

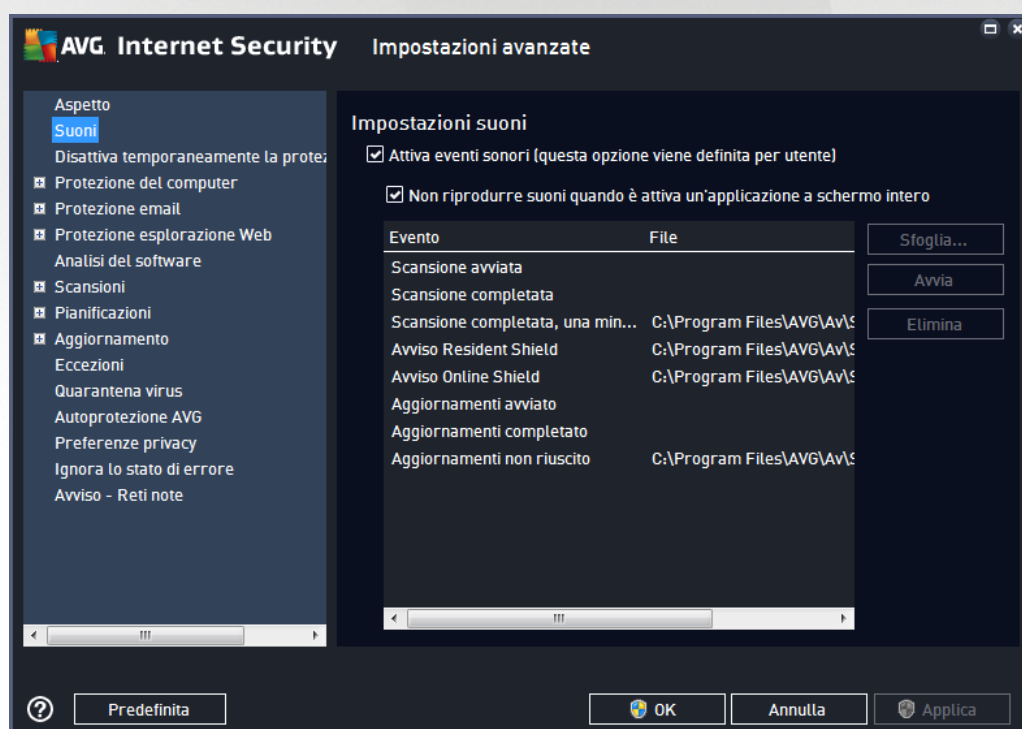
- o **Notifiche statistiche** (attivata per impostazione predefinita) - consente di decidere se visualizzare le notifiche relative alle revisioni statistiche regolari nell'area di notifica.
- o **Notifiche per AVG Advisor** (attivata per impostazione predefinita) - consente di decidere se visualizzare le informazioni relative alle attività di [AVG Advisor](#) in una finestra a comparsa nell'area di notifica.

### Modalità gioco

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

### 3.5.2. Suoni

Nella finestra di dialogo **Impostazioni audio** è possibile specificare se si desidera essere informati circa specifiche azioni di **AVG Internet Security** tramite una notifica sonora:



Le impostazioni sono valide solo per l'account utente corrente, pertanto ogni utente del computer può disporre di impostazioni personalizzate per i suoni. Per consentire le notifiche sonore, mantenere l'opzione **Attiva eventi sonori** selezionata (l'opzione è attivata per impostazione predefinita) per attivare l'elenco di tutte le azioni correlate. Inoltre, è possibile selezionare l'opzione **Non riprodurre suoni quando è attiva un'applicazione a schermo intero** per eliminare le notifiche sonore quando potrebbero essere di disturbo (vedere anche la sezione relativa alla modalità gioco del capitolo [Impostazioni avanzate/Aspetto](#) in questo





documento).

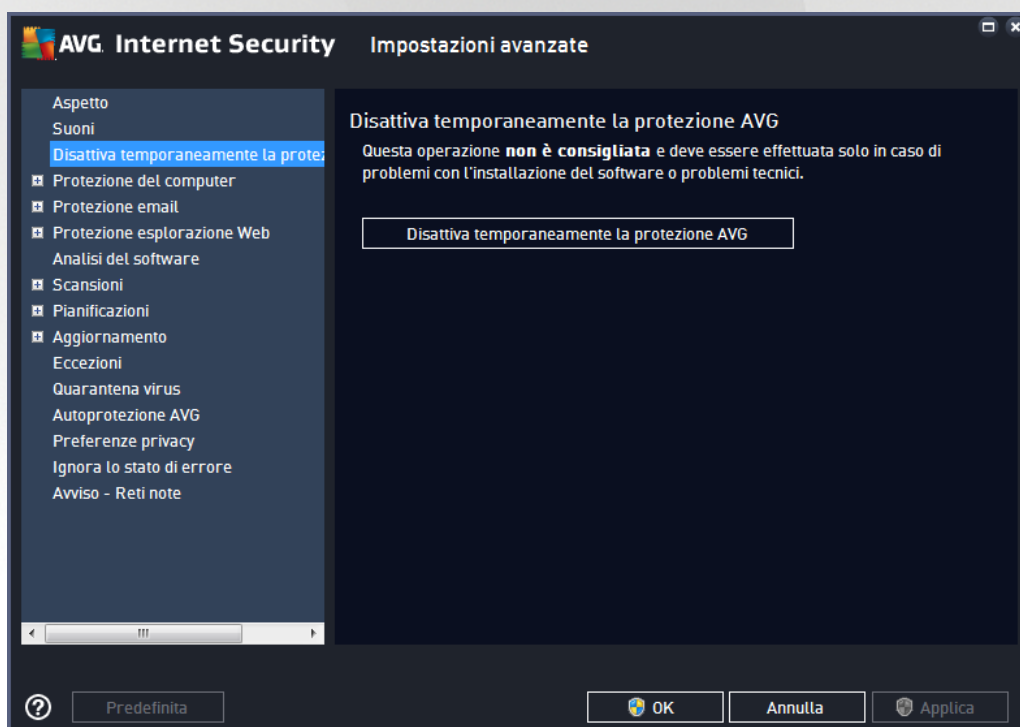
### Pulsanti di controllo

- **Sfoglia...** - dopo aver selezionato l'evento dall'elenco, utilizzare il pulsante **Sfoglia** per ricercare nel disco il file audio desiderato da assegnare all'evento (*al momento sono supportati solo file \*.wav*).
- **Avvia** - per ascoltare il suono selezionato, evidenziare l'evento nell'elenco e fare clic sul pulsante **Avvia**.
- **Elimina** - utilizzare il pulsante **Elimina** per rimuovere il suono assegnato a uno specifico evento.

### 3.5.3. Disattivazione temporanea della protezione di AVG

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

**Non utilizzare questa opzione se non è assolutamente necessario.**

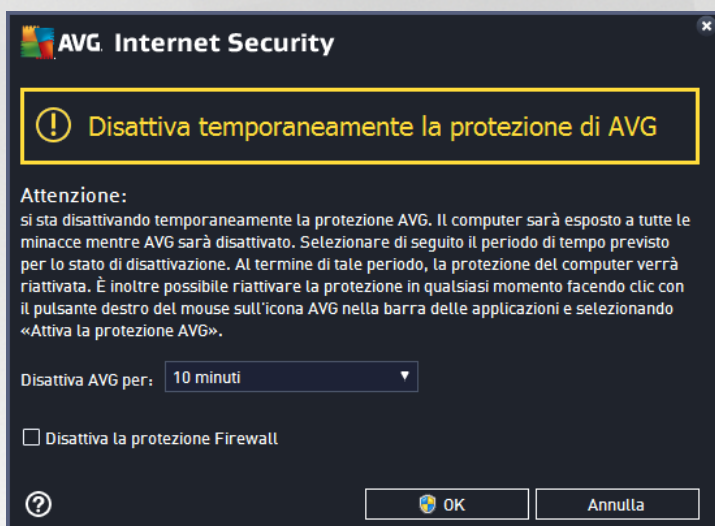


Nella maggior parte dei casi, **non è necessario** disattivare **AVG Internet Security** prima di installare nuovi software o driver, neppure se il programma di installazione o la procedura guidata suggeriscono di chiudere tutti i programmi e le applicazioni in esecuzione per accertarsi che non si verifichino interruzioni indesiderate durante il processo di installazione. In caso di problemi durante l'installazione, provare innanzitutto a [disattivare la protezione permanente](#) (nella finestra di dialogo collegata *deselezionare la voce **Abilita Resident Shield***). Se fosse necessario disattivare temporaneamente **AVG Internet Security**, lo si dovrà riattivare non appena possibile. Se si è connessi a Internet o a una rete mentre il software antivirus è disattivato, il computer sarà esposto a potenziali attacchi.



## Come disattivare la protezione AVG

Selezionare la casella di controllo **Disattiva temporaneamente la protezione di AVG** e confermare la scelta facendo clic sul pulsante **Applica**. Nella finestra di dialogo **Disattiva temporaneamente la protezione di AVG** aperta specificare per quanto tempo si desidera disattivare **AVG Internet Security**. Per impostazione predefinita, la protezione verrà disattivata per 10 minuti, tempo sufficiente per svolgere attività comuni quali l'installazione di un nuovo software e così via. È possibile impostare un periodo di tempo più lungo, tuttavia si consiglia di non utilizzare questa opzione se non è assolutamente necessario. Successivamente, tutti i componenti disattivati verranno riattivati automaticamente. È comunque possibile disattivare la protezione di AVG fino al successivo riavvio del computer. Un'opzione distinta per disattivare il componente **Firewall** è presente nella finestra di dialogo **Disattiva temporaneamente la protezione di AVG**. Per eseguire questa operazione, selezionare **Disattiva la protezione Firewall**.

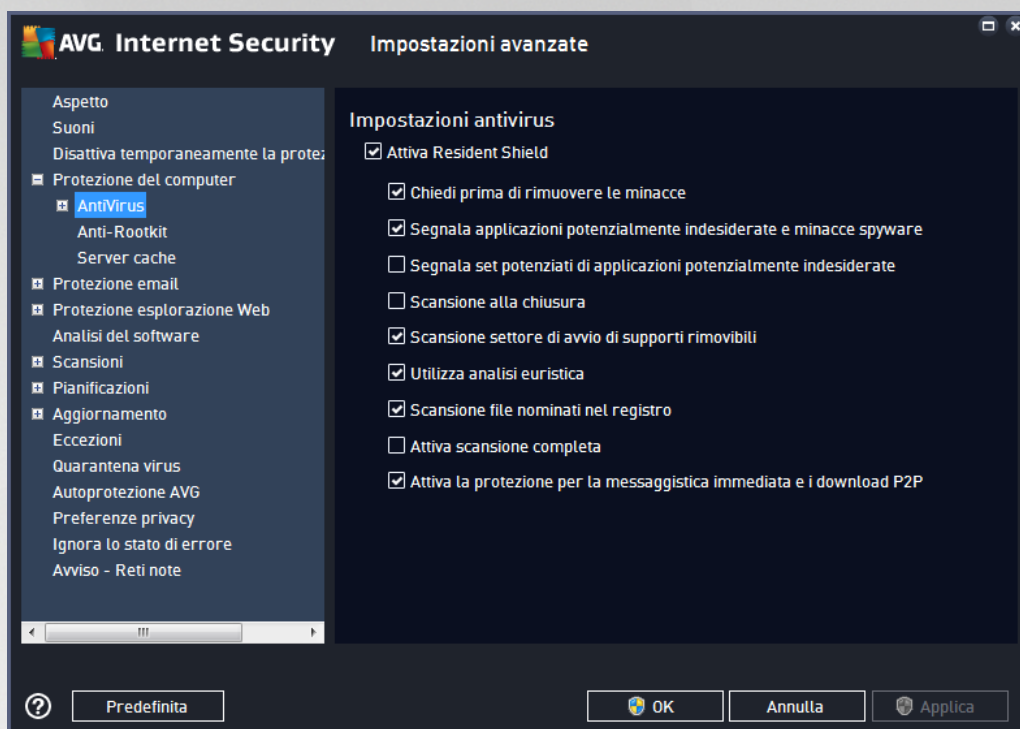


## 3.5.4. Protezione del computer

### 3.5.4.1. AntiVirus

**AntiVirus** e **Resident Shield** proteggono il computer in modo continuo da tutti i tipi noti di virus, spyware e malware in generale (*inclusi i cosiddetti malware dormienti e inattivi, ovvero i malware scaricati ma non ancora attivati*).





Nella finestra di dialogo **Impostazioni di Resident Shield** è possibile attivare o disattivare completamente la protezione permanente selezionando/deselezionando la voce **Attiva Resident Shield** (attivata per impostazione predefinita). Inoltre, è possibile selezionare quali funzionalità della protezione permanente devono essere attivate:

- **Chiedi prima di rimuovere le minacce** (attivata per impostazione predefinita) - selezionando questa opzione, Resident Shield non eseguirà alcuna azione automaticamente. Verrà invece visualizzata una finestra di dialogo che descrive la minaccia rilevata, consentendo di scegliere l'azione da eseguire. Se si mantiene deselezionata la casella, **AVG Internet Security** tenterà automaticamente di correggere l'infezione e, nel caso sia impossibile, sposterà l'oggetto in [Quarantena virus](#).
- **Segnala applicazioni potenzialmente indesiderate e minacce spyware** (attivata per impostazione predefinita) - selezionare questa casella di controllo per attivare la scansione per ricercare spyware e virus. Gli spyware rappresentano una categoria di malware anomala: anche se solitamente costituiscono un rischio per la sicurezza, alcuni di questi programmi possono essere installati intenzionalmente. Si consiglia di mantenere questa funzionalità attivata in quanto consente di aumentare la protezione del computer.
- **Segnala set potenziati di applicazioni potenzialmente indesiderate** (disattivata per impostazione predefinita) - selezionare questa casella di controllo per rilevare pacchetti estesi di spyware, ovvero programmi perfettamente normali e innocui al momento dell'acquisto diretto presso il produttore, ma utilizzabili a scopi dannosi successivamente. Si tratta di una precauzione aggiuntiva che aumenta ulteriormente la protezione del computer, ma che potrebbe bloccare programmi legittimi, pertanto l'opzione è disattivata per impostazione predefinita.
- **Scansione alla chiusura** (disattivata per impostazione predefinita) - la scansione alla chiusura assicura che AVG esegua la scansione di oggetti attivi (ad esempio applicazioni, documenti e così via) quando vengono aperti e anche quando vengono chiusi. Questa funzionalità consente di proteggere il computer da alcuni tipi di virus sofisticati.



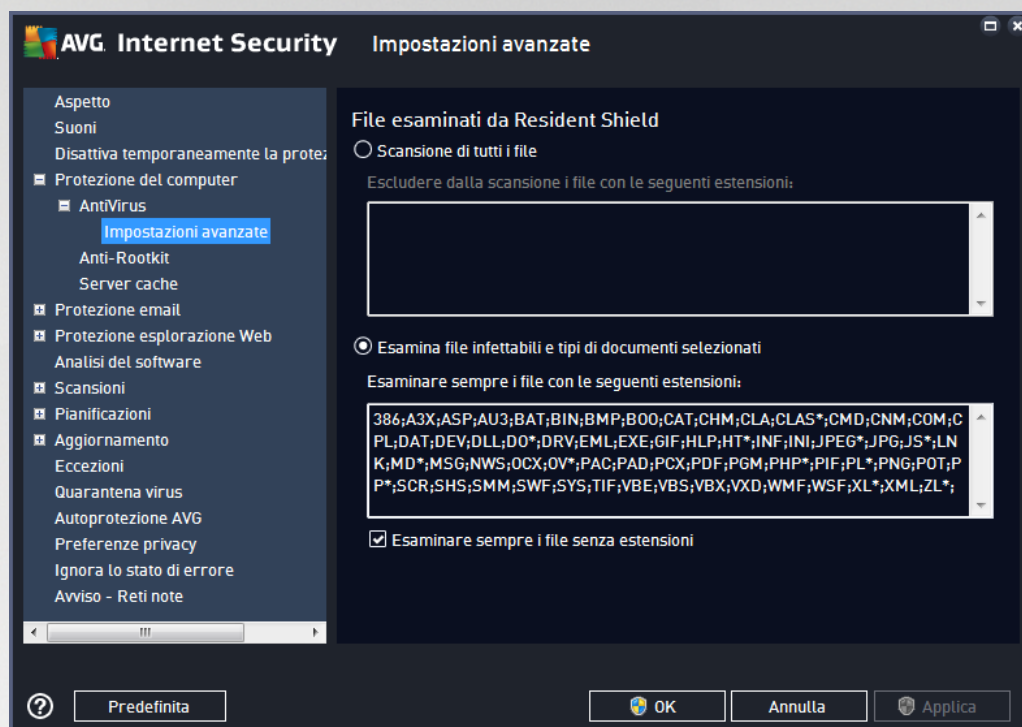
- **Scansione settore di avvio di supporti rimovibili** (attivata per impostazione predefinita): selezionare questa casella di controllo per eseguire la scansione del settore di avvio dei dischi flash USB, dei dischi rigidi esterni e di altri supporti rimovibili per accertarsi che non contengano minacce.
- **Usa analisi euristiche** (attivata per impostazione predefinita): l'analisi euristica verrà utilizzata per il rilevamento (*emulazione dinamica delle istruzioni dell'oggetto sottoposto a scansione in un ambiente informatico virtuale*).
- **Scansione file nominati nel registro** (attivata per impostazione predefinita): questo parametro specifica che AVG sottoporrà a scansione tutti i file eseguibili aggiunti al registro di avvio per evitare che un'infezione nota venga eseguita al successivo avvio del computer.
- **Attiva scansione completa** (disattivata per impostazione predefinita) : in situazioni specifiche (*stati di estrema emergenza*) è possibile selezionare questa opzione per attivare gli algoritmi di scansione più completi che esamineranno accuratamente tutti gli oggetti potenzialmente minacciosi. Tenere presente tuttavia che questo metodo è piuttosto dispendioso in termini di tempo.
- **Attiva la protezione per la messaggistica immediata e i download P2P** (attivata per impostazione predefinita) : selezionare questa voce se si desidera verificare che la comunicazione tramite messaggistica immediata (*ad esempio AIM, Yahoo!, ICQ, Skype, MSN Messenger e così via*) e i dati scaricati nelle reti peer-to-peer (*reti potenzialmente pericolose che consentono la connessione diretta tra client, senza un server, in genere sono utilizzate per condividere file musicali*) siano privi di virus.

**Nota:** se AVG è installato in Windows 10, nell'elenco è presente un altro elemento denominato **Attivare Windows Antimalware Scan Interface (AMSI) per scansioni del software più approfondite**. Questa funzionalità ottimizza la protezione antivirus e consente a Windows e ad AVG di cooperare per rendere la protezione più affidabile e ridurre il numero di falsi positivi.





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

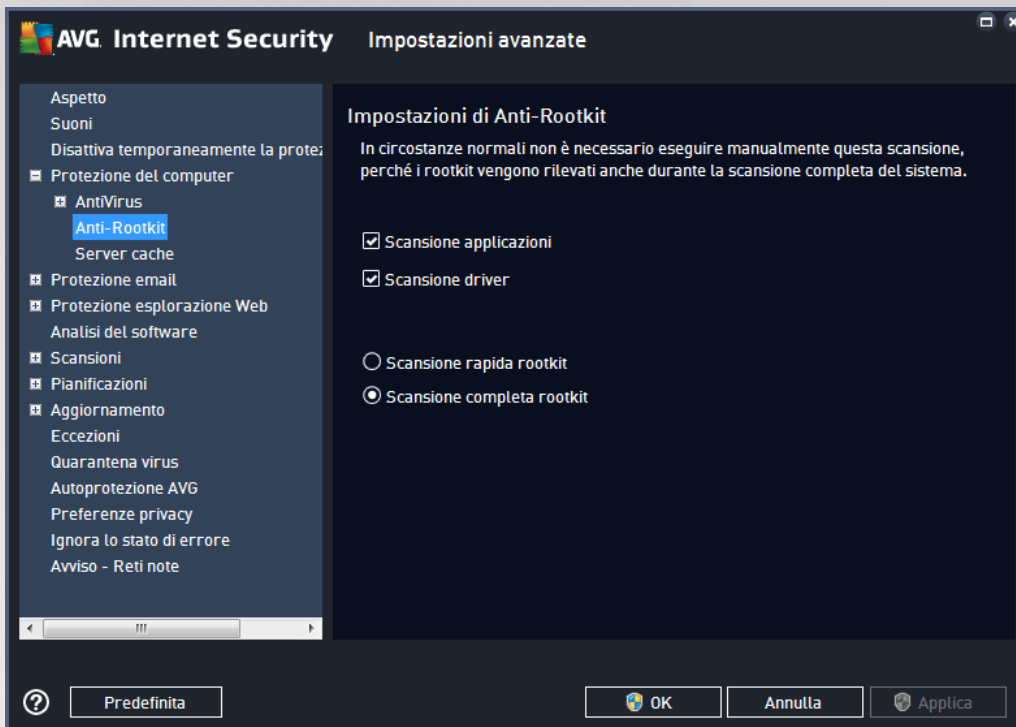


Selezionare la casella di controllo pertinente per specificare se si desidera utilizzare l'opzione **Scansione di tutti i file** oppure l'opzione **Esamina file infettabili e tipi di documenti selezionati**. Per velocizzare la scansione e assicurare contemporaneamente il livello massimo di protezione, si consiglia di mantenere le impostazioni predefinite. In questo modo verranno sottoposti a scansione solo i file infettabili. Nella relativa sezione della finestra di dialogo è inoltre possibile trovare un elenco modificabile delle estensioni che definiscono i file inclusi nella scansione.

Selezionare l'opzione **Esaminare sempre i file senza estensioni** (*attivata per impostazione predefinita*) per assicurare che Resident Shield esegua anche la scansione dei file senza estensione e di formato sconosciuto. Si consiglia di mantenere questa funzionalità sempre attivata, in quanto i file senza estensione sono sospetti.

### 3.5.4.2. Anti-Rootkit

Nella finestra di dialogo **Impostazioni di Anti-Rootkit** è possibile modificare la configurazione del servizio **Anti-Rootkit** e i parametri specifici della scansione Anti-Rootkit. La scansione Anti-Rootkit è un processo predefinito incluso nella [Scansione intero computer](#):



**Scansione applicazioni** e **Scansione driver** consentono di specificare in dettaglio gli elementi da includere nella scansione Anti-Rootkit. Queste impostazioni sono progettate per utenti esperti. Si consiglia di lasciare attivate tutte le opzioni. È inoltre possibile selezionare la modalità di scansione rootkit:

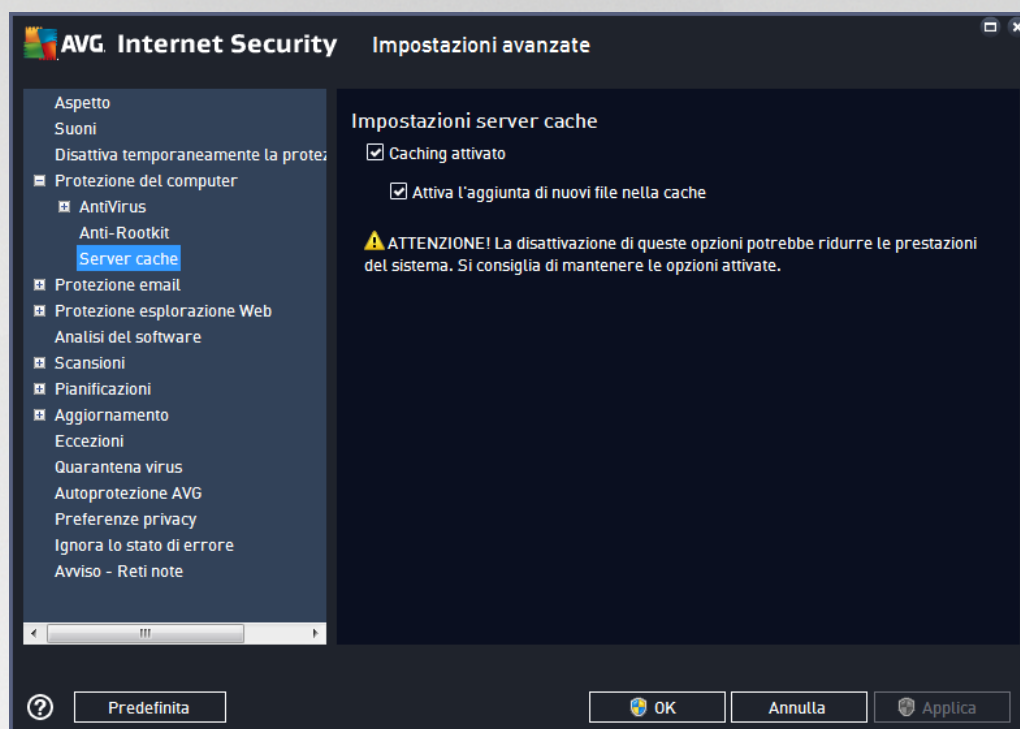
- **Scansione rapida rootkit** - sottopone a scansione tutti i processi in esecuzione, i driver caricati e la cartella di sistema (*solitamente c:\Windows*)
- **Scansione completa rootkit** - sottopone a scansione tutti i processi in esecuzione, i driver caricati e la cartella di sistema (*solitamente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





### 3.5.4.3. Server cache

La finestra di dialogo **Impostazioni del Server cache** si riferisce al processo server cache destinato a velocizzare tutti i tipi di scansione di **AVG Internet Security**:



Il server cache raccoglie e mantiene le informazioni relative ai file affidabili (*un file viene considerato affidabile se presenta la firma digitale di una fonte affidabile*). Questi file vengono quindi considerati sicuri e non necessitano di ulteriore scansione, pertanto vengono ignorati durante le scansioni.

La finestra di dialogo **Impostazioni del Server cache** offre le seguenti opzioni di configurazione:

- **Caching attivato** (*attivata per impostazione predefinita*) - deselezionare la casella per disattivare il **Server cache** e svuotare la memoria cache. Tenere presente che la scansione potrebbe subire un rallentamento e le prestazioni complessive del computer potrebbero ridursi, poiché per prima cosa ogni singolo file in uso verrà sottoposto alla scansione antivirus e antispyware.
- **Attiva l'aggiunta di nuovi file nella cache** (*attivata per impostazione predefinita*) - deselezionare la casella per arrestare l'aggiunta di ulteriori file nella memoria cache. Tutti i file già presenti nella cache verranno mantenuti e utilizzati finché l'inserimento nella cache non verrà disattivato completamente o finché non verrà eseguito il successivo aggiornamento del database dei virus.

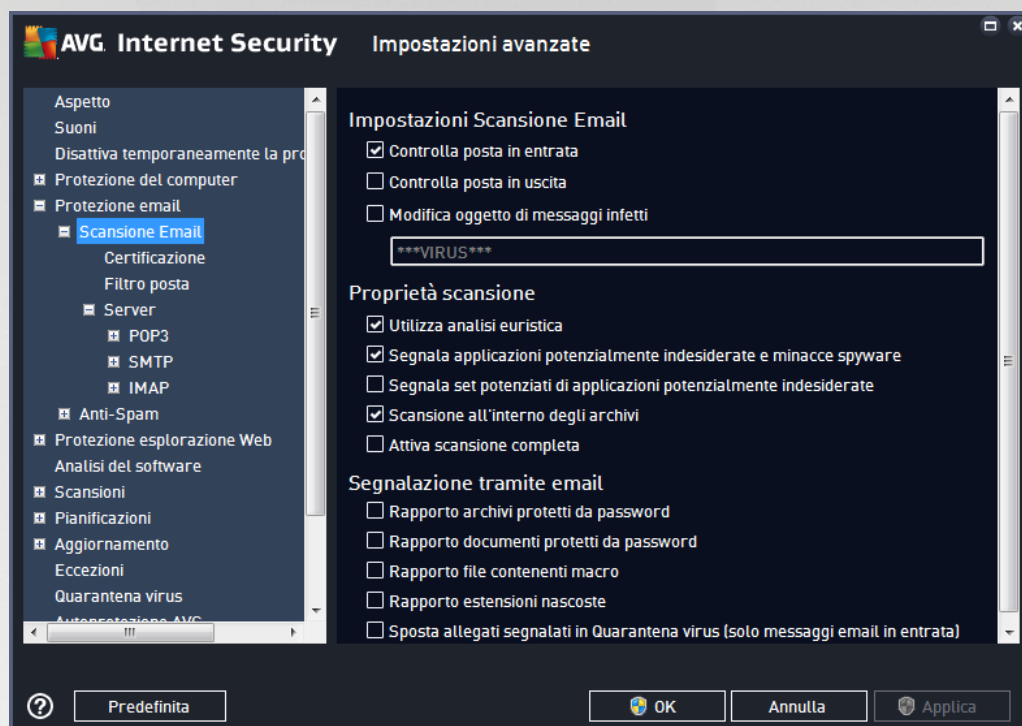
***A meno che non sussista un motivo valido per disattivare il server cache, si consiglia di mantenere le impostazioni predefinite e lasciare attivate entrambe le opzioni. In caso contrario, la velocità e le prestazioni del sistema potrebbero ridursi notevolmente.***

### 3.5.5. Scansione Email

In questa sezione è possibile modificare la configurazione dettagliata di [Scansione Email](#) e [Anti-Spam](#):

### 3.5.5.1. Scansione Email

La finestra di dialogo **Scansione Email** è suddivisa in tre sezioni:



#### Scansione dell'email

In questa sezione è possibile configurare le seguenti impostazioni di base per i messaggi email in arrivo e/o in uscita:

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

#### Proprietà scansione

In questa sezione è possibile specificare la modalità di scansione dei messaggi email:

- **Usa analisi euristiche** (attivata per impostazione predefinita) - selezionare questa opzione per utilizzare il metodo di rilevamento tramite analisi euristica durante la scansione dei messaggi email. Se questa opzione è attivata, è possibile filtrare gli allegati dei messaggi email non solo per estensione ma anche in base al contenuto effettivo dell'allegato. Il filtro può essere impostato nella finestra di dialogo [Filtro posta](#).





- **Segnala applicazioni potenzialmente indesiderate e minacce spyware** (attivata per impostazione predefinita) - selezionare questa casella di controllo per attivare la scansione per ricercare spyware e virus. Gli spyware rappresentano una categoria di malware anomala: anche se solitamente costituiscono un rischio per la sicurezza, alcuni di questi programmi possono essere installati intenzionalmente. Si consiglia di mantenere questa funzionalità attivata in quanto consente di aumentare la protezione del computer.
- **Segnala set potenziati di applicazioni potenzialmente indesiderate** (disattivata per impostazione predefinita) - selezionare questa casella di controllo per rilevare pacchetti estesi di spyware, ovvero programmi perfettamente normali e innocui al momento dell'acquisto diretto presso il produttore, ma utilizzabili a scopi dannosi successivamente. Si tratta di una precauzione aggiuntiva che aumenta ulteriormente la protezione del computer, ma che potrebbe bloccare programmi legittimi, pertanto l'opzione è disattivata per impostazione predefinita.
- **Scansione all'interno degli archivi** (attivata per impostazione predefinita) - selezionare questa casella di controllo per eseguire la scansione del contenuto degli archivi allegati ai messaggi email.
- **Attiva scansione completa** (disattivata per impostazione predefinita) - in situazioni specifiche (ad esempio se si sospetta che il computer sia stato infettato da un virus o un attacco) per maggiore sicurezza è possibile selezionare questa opzione per attivare gli algoritmi di scansione più completi che esamineranno anche le aree del computer che difficilmente vengono infettate. Tenere presente tuttavia che questo metodo è piuttosto dispendioso in termini di tempo.

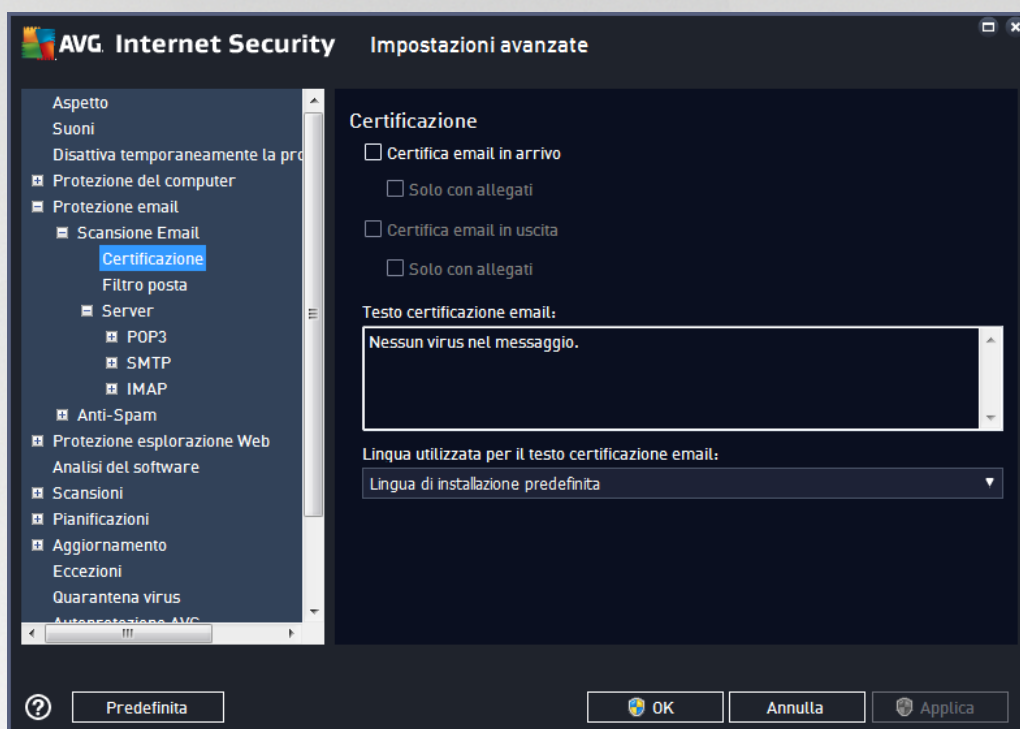
### Segnalazione allegati email

In questa sezione, è possibile impostare rapporti aggiuntivi sui file potenzialmente pericolosi o sospetti. Tenere presente che non verrà visualizzato alcun messaggio di avviso, verrà aggiunto soltanto un testo di certificazione alla fine del messaggio email e tutti i rapporti verranno elencati nella finestra di dialogo [Rilevamento Protezione email](#):

- **Segnala archivi protetti da password** - gli archivi (ZIP, RAR e così via) protetti da password non possono essere sottoposti alla scansione antivirus. Selezionare la casella di controllo se si desidera che questi file vengano segnalati come potenzialmente pericolosi.
- **Segnala documenti protetti da password** - i documenti protetti da password non possono essere sottoposti alla scansione antivirus. Selezionare la casella di controllo se si desidera che questi file vengano segnalati come potenzialmente pericolosi.
- **Segnala file contenenti macro** - una macro è una sequenza di passaggi predefinita che consente di semplificare determinate attività (le macro di MS Word, ad esempio, sono ampiamente conosciute). Le macro possono contenere istruzioni potenzialmente pericolose. Selezionare la casella di controllo per assicurare che i file contenenti macro vengano segnalati come potenzialmente pericolosi.
- **Segnala estensioni nascoste** - le estensioni nascoste possono far sembrare un file sospetto, ad esempio un file eseguibile del tipo "nomefile.txt.exe", come un innocuo file di testo del tipo "nomefile.txt". Selezionare la casella di controllo se si desidera che questi file vengano segnalati come potenzialmente pericolosi.
- **Sposta allegati segnalati in Quarantena virus** - consente di specificare se si desidera ricevere una notifica via email per gli archivi protetti da password, i documenti protetti da password, i file contenenti macro e/o i file con estensione nascosta rilevati come allegato del messaggio email sottoposto a scansione. Se viene identificato un messaggio simile durante la scansione, è possibile stabilire se l'oggetto infetto rilevato deve essere spostato in [Quarantena virus](#).



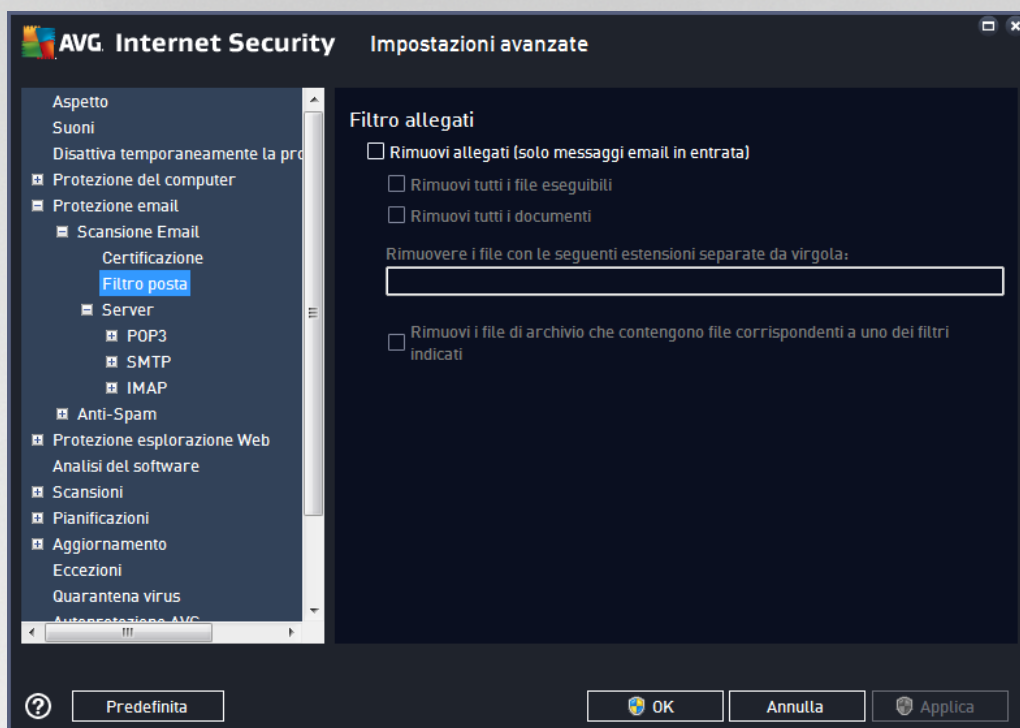
Nella finestra di dialogo **Certificazione** è possibile selezionare le caselle di controllo specifiche per specificare se si desidera certificare la posta in arrivo (**Certifica email in arrivo**) e/o la posta in uscita (**Certifica email in uscita**). Per ciascuna di queste opzioni è inoltre possibile specificare il parametro **Solo con allegati** per far sì che la certificazione venga aggiunta solo ai messaggi email con allegati:



Per impostazione predefinita, il testo di certificazione è composto da informazioni di base simili a *Nessun virus in questo messaggio*. Tuttavia, è possibile estendere o modificare queste informazioni in base alle esigenze, scrivendo il testo di certificazione desiderato nel campo **Testo certificazione email**. Nella sezione **Lingua utilizzata per il testo certificazione email** è possibile inoltre definire in quale lingua verrà visualizzata la parte di certificazione generata automaticamente (*Nessun virus in questo messaggio*).

**Nota:** tenere presente che solo il testo predefinito verrà visualizzato nella lingua richiesta e il testo personalizzato non verrà tradotto automaticamente.





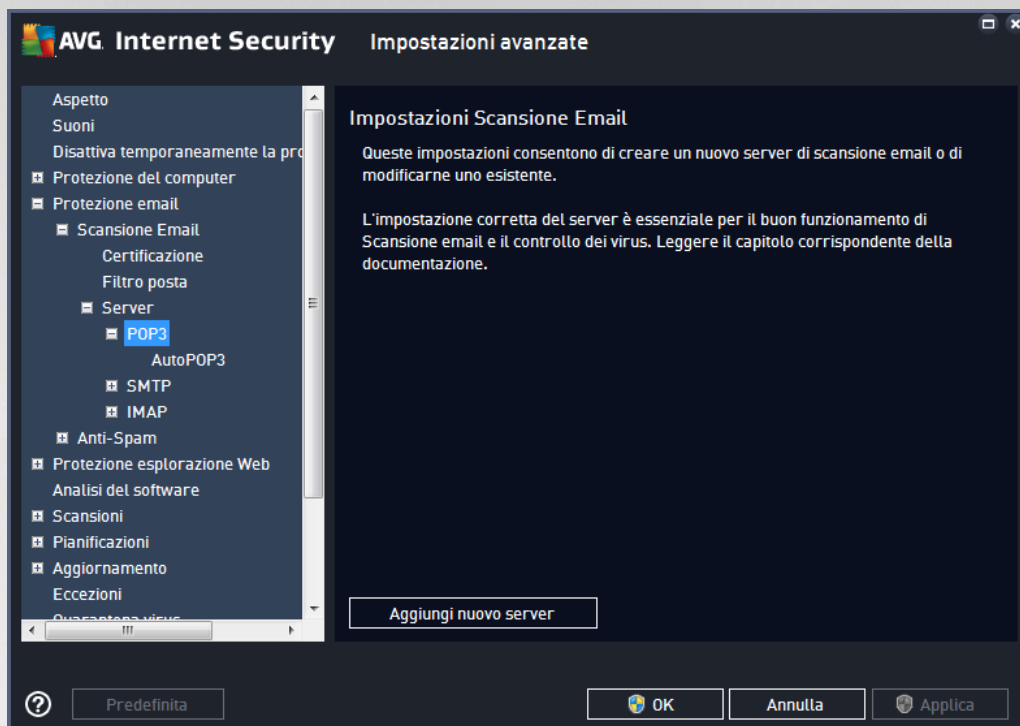
La finestra di dialogo **Filtro allegati** consente di impostare i parametri per la scansione degli allegati ai messaggi email. Per impostazione predefinita, l'opzione **Rimuovi allegati** è disattivata. Se si decide di attivarla, tutti gli allegati ai messaggi email rilevati come infetti o potenzialmente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

- **Rimuovi tutti i file eseguibili** - tutti i file \*.exe verranno eliminati
- **Rimuovi tutti i documenti** - tutti i file \*.doc, \*.docx, \*.xls e \*.xlsx verranno eliminati
- **Rimuovere i file con le seguenti estensioni separate da virgola** - verranno rimossi tutti i file con le estensioni specificate

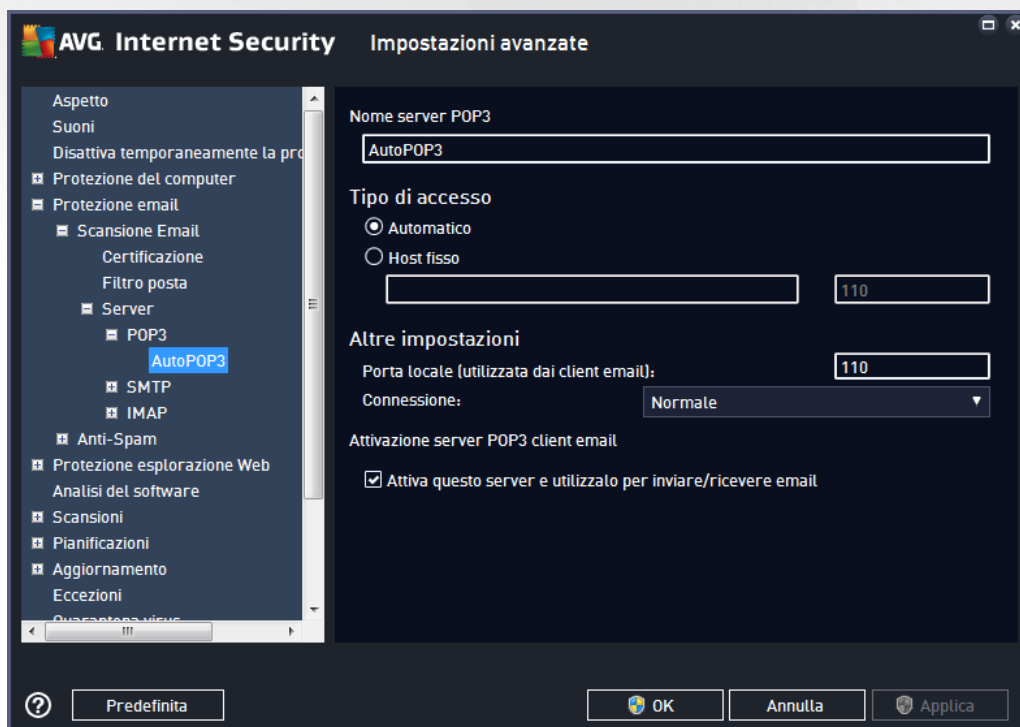
Nella sezione **Server** è possibile modificare i parametri dei server di [Scansione Email](#):

- [Server POP3](#)
- [Server SMTP](#)
- [Server IMAP](#)

Inoltre, è possibile definire nuovi server per la posta in arrivo o in uscita, utilizzando il pulsante **Aggiungi nuovo server**.



Questa finestra di dialogo consente di impostare un nuovo server [Scansione Email](#) che utilizza il protocollo POP3 per la posta in entrata:



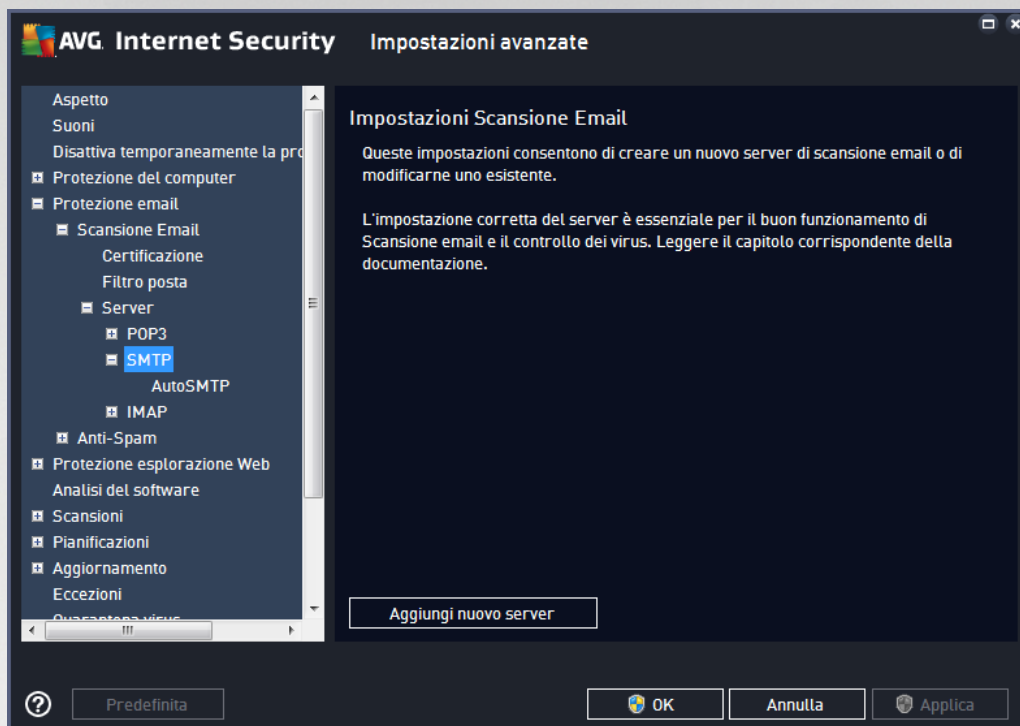
- **Nome server POP3** - in questo campo è possibile specificare il nome dei nuovi server aggiunti (per



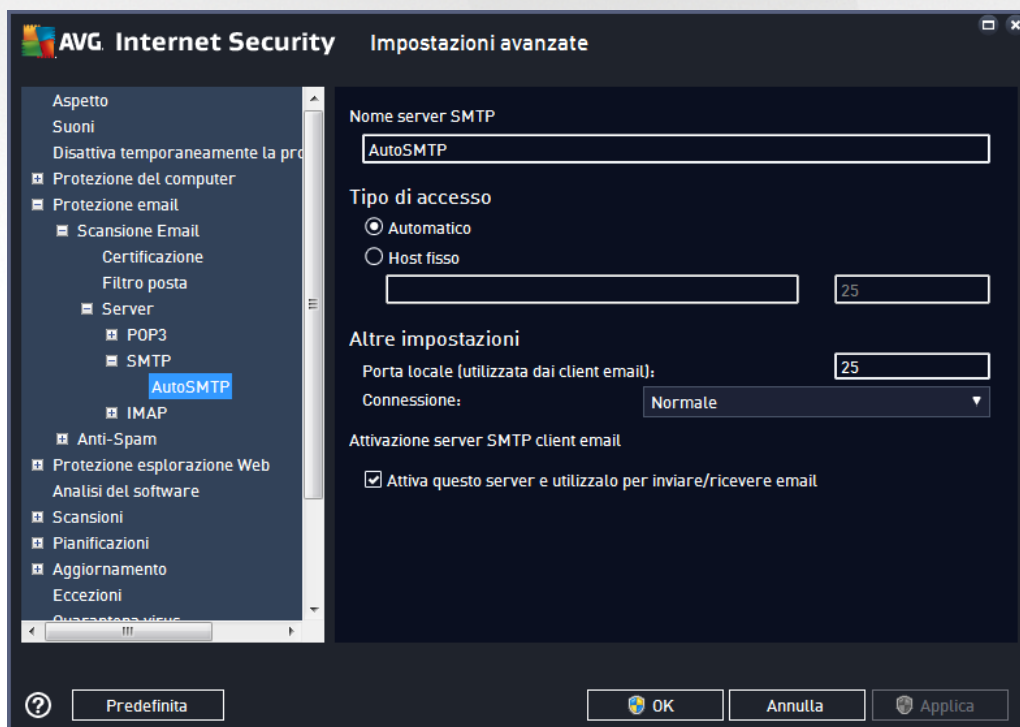


aggiungere un server POP3, fare clic con il pulsante destro del mouse sulla voce POP3 nel menu di esplorazione a sinistra).

- **Tipo di accesso** - definisce il metodo per determinare il server email utilizzato per la posta in entrata:
  - **Automatico** - l'accesso verrà effettuato automaticamente, in base alle impostazioni del client email.
  - **Host fisso** - in questo caso verrà sempre utilizzato il server specificato in questo campo. Specificare l'indirizzo o il nome del server di posta. Il nome di accesso non verrà modificato. Per il nome, è possibile utilizzare un nome di dominio (*ad esempio pop.acme.com*) o un indirizzo IP (*ad esempio 123.45.67.89*). Se il server email utilizza una porta non standard, è possibile specificare il nome della porta dopo quello del server utilizzando come separatore il segno di due punti (*ad esempio pop.acme.com:8200*). La porta standard per la comunicazione POP3 è la numero 110.
- **Altre impostazioni** - specifica parametri più dettagliati:
  - **Porta locale** - specifica la porta su cui è prevista la comunicazione dall'applicazione email. Nell'applicazione email sarà quindi necessario specificare tale porta come porta per la comunicazione POP3.
  - **Connessione** - nel menu a discesa è possibile specificare il tipo di connessione da utilizzare (*regolare/SSL/SSL predefinito*). Se si sceglie la connessione SSL, i dati inviati verranno crittografati senza il rischio di essere rilevati o monitorati da terzi. Questa funzionalità è disponibile solo se supportata dal server email di destinazione.
- **Attivazione server POP3 client email** - selezionare/deselezionare questa voce per attivare o disattivare il server POP3 specificato



Questa finestra di dialogo consente di impostare un nuovo server [Scansione Email](#) che utilizza il protocollo SMTP per la posta in uscita:



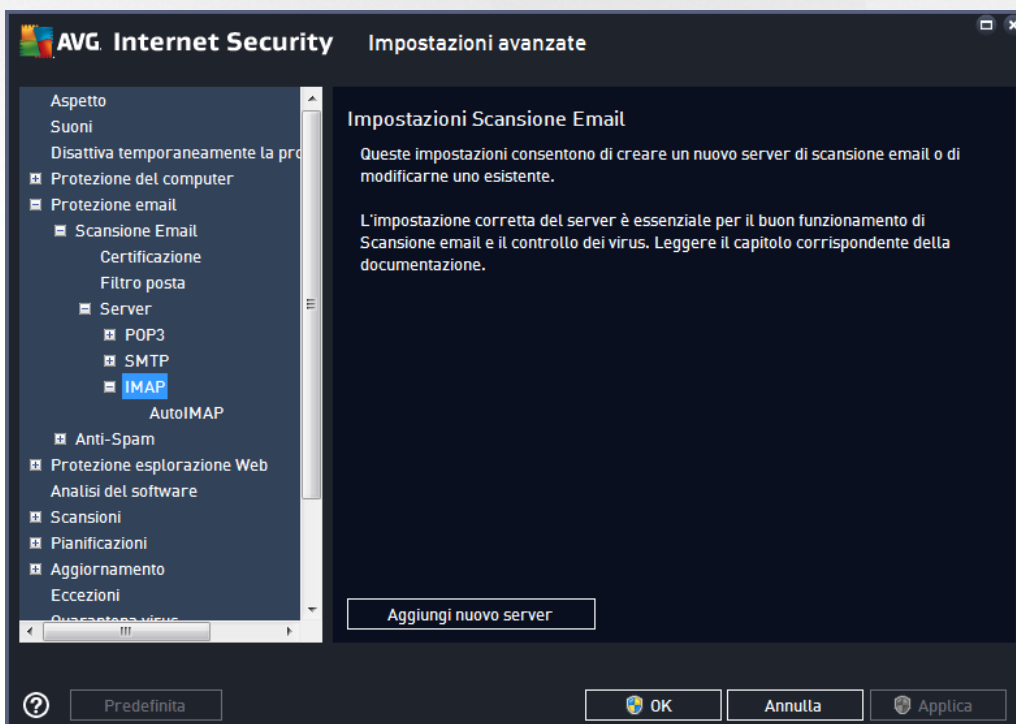
- **Nome server SMTP** - in questo campo è possibile specificare il nome dei nuovi server aggiunti (per





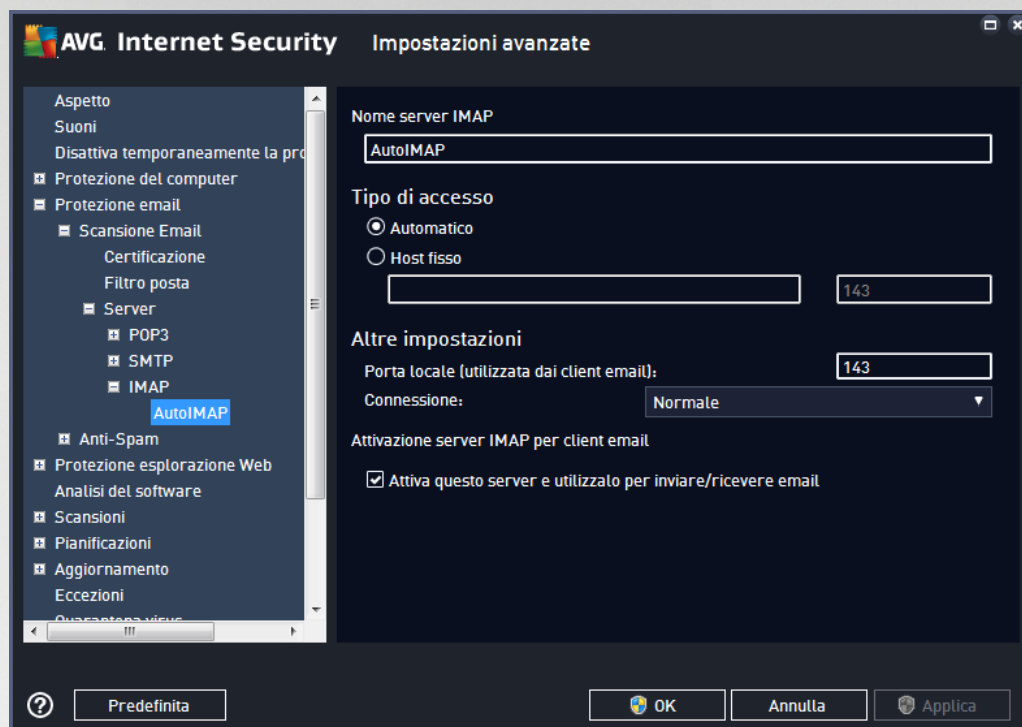
aggiungere un server SMTP, fare clic con il pulsante destro del mouse sulla voce SMTP nel menu di esplorazione a sinistra). Per i server "AutoSMTP" creati automaticamente questo campo è disattivato.

- **Tipo di accesso** - definisce il metodo per determinare il server email utilizzato per la posta in uscita:
  - **Automatico** - l'accesso verrà effettuato automaticamente, in base alle impostazioni del client email
  - **Host fisso** - in questo caso verrà sempre utilizzato il server specificato in questo campo. Specificare l'indirizzo o il nome del server di posta. Per il nome, è possibile utilizzare un nome di dominio (*ad esempio smtp.acme.com*) o un indirizzo IP (*ad esempio 123.45.67.89*). Se il server email utilizza una porta non standard, è possibile digitare il nome della porta dopo quello del server utilizzando come separatore il segno di due punti, *ad esempio smtp.acme.com:8200*. La porta standard per la comunicazione SMTP è la numero 25.
- **Altre impostazioni** - specifica parametri più dettagliati:
  - **Porta locale** - specifica la porta su cui è prevista la comunicazione dall'applicazione email. Nell'applicazione email sarà quindi necessario specificare tale porta come porta per la comunicazione SMTP.
  - **Connessione** - questo menu a discesa consente di specificare il tipo di connessione da utilizzare (*normale/SSL/SSL predefinito*). Se si sceglie la connessione SSL, i dati inviati verranno crittografati senza il rischio di essere rilevati o monitorati da terzi. Questa funzionalità è disponibile solo se supportata dal server email di destinazione.
- **Attivazione server SMTP per client email** - selezionare/deselezionare questa casella per attivare/disattivare il server SMTP specificato sopra





Questa finestra di dialogo consente di impostare un nuovo server [Scansione Email](#) che utilizza il protocollo IMAP per la posta in uscita:



- **Nome server IMAP** - in questo campo è possibile specificare il nome dei nuovi server aggiunti (per aggiungere un server IMAP, fare clic con il pulsante destro del mouse sulla voce IMAP nel menu di esplorazione a sinistra).
- **Tipo di accesso** - definisce il metodo per determinare il server email utilizzato per la posta in uscita:
  - **Automatico** - l'accesso verrà effettuato automaticamente, in base alle impostazioni del client email
  - **Host fisso** - in questo caso verrà sempre utilizzato il server specificato in questo campo. Specificare l'indirizzo o il nome del server di posta. Per il nome, è possibile utilizzare un nome di dominio (ad esempio *smtp.acme.com*) o un indirizzo IP (ad esempio *123.45.67.89*). Se il server email utilizza una porta non standard, è possibile digitare il nome della porta dopo quello del server utilizzando come separatore il segno di due punti, ad esempio *imap.acme.com:8200*. La porta standard per la comunicazione IMAP è la numero 143.
- **Altre impostazioni** - specifica parametri più dettagliati:
  - **Porta locale** - specifica la porta su cui è prevista la comunicazione dall'applicazione email. Nell'applicazione email sarà quindi necessario specificare tale porta come porta per la comunicazione IMAP.
  - **Connessione** - questo menu a discesa consente di specificare il tipo di connessione da utilizzare (*normale/SSL/SSL predefinito*). Se si sceglie la connessione SSL, i dati inviati verranno crittografati senza il rischio di essere rilevati o monitorati da terze parti. Questa funzionalità è disponibile solo se supportata dal server email di destinazione.





- **Attivazione server IMAP per client email** - selezionare/deselezionare questa casella per attivare/disattivare il server IMAP specificato sopra

### 3.5.5.2. Anti-Spam

Nella finestra di dialogo delle **impostazioni Anti-Spam** è possibile selezionare/deselezionare la casella di controllo **Attiva protezione Anti-Spam** per consentire/impedire la scansione anti-spam delle comunicazioni email. Questa opzione è attivata per impostazione predefinita e si consiglia di non modificare questa impostazione a meno che non siano presenti motivi validi per farlo.

Quindi, è anche possibile selezionare il grado di "aggressività" della configurazione del conteggio. Il filtro **Anti-Spam** assegna a ciascun messaggio un conteggio (*ad esempio, il grado di somiglianza del contenuto del messaggio con lo SPAM*) in base a diverse tecniche di scansione dinamica. Per modificare l'impostazione **Contrassegna messaggio come spam se il conteggio è maggiore di**, digitare un valore oppure spostare il dispositivo di scorrimento a destra o a sinistra.

L'intervallo di valori è compreso tra 50 e 90. Di seguito viene fornita una panoramica generale della soglia di conteggio:

- **Valore compreso tra 80 e 90** - verranno filtrati i messaggi email il cui contenuto è probabilmente spam, ma potrebbero essere filtrati anche alcuni messaggi che non ne contengono.
- **Valore tra 60 e 79** - è considerata una configurazione abbastanza "aggressiva". Verranno filtrati i messaggi email il cui contenuto potrebbe essere spam, ma potrebbero essere filtrati anche messaggi che non ne contengono.
- **Valore tra 50 e 59** - configurazione particolarmente aggressiva. È probabile che insieme ai messaggi email contenenti spam vengano filtrati anche i messaggi normali. **Questo intervallo di valori non è consigliato.**

Nella finestra di dialogo delle **impostazioni Anti-Spam** è possibile definire ulteriormente la modalità di gestione dei messaggi email di spam:

- **Sposta messaggio nella cartella della posta indesiderata** (solo plug-in Microsoft Outlook) - selezionare questa casella di controllo per specificare che ciascun messaggio di spam rilevato deve essere automaticamente spostato nella cartella specifica della posta indesiderata all'interno del client email Microsoft Outlook. Al momento, questa funzione non è supportata in altri client email.
- **Aggiungi destinatari delle email inviate alla [whitelist](#)** - selezionare questa casella di controllo per confermare che tutti i destinatari delle email inviate sono affidabili e tutte le email provenienti dai relativi account email possono essere recapitate.
- **Modifica oggetto per messaggi contrassegnati come SPAM** - selezionare questa casella di controllo se si desidera che tutti i messaggi rilevati come spam vengano contrassegnati con una parola o un carattere specifico nel campo dell'oggetto del messaggio email. Il testo desiderato può essere digitato nel campo di testo attivato.
- **Chiedi conferma prima di segnalare rilevamenti errati** - se durante il processo di installazione si è scelto di partecipare al progetto [Preferenze privacy](#), si è acconsentito a segnalare le minacce rilevate a AVG. Il rilevamento viene eseguito automaticamente. È tuttavia possibile selezionare questa casella di controllo per specificare se si desidera che venga richiesta una conferma prima della segnalazione ad AVG dell'eventuale spam rilevato, in modo da assicurarsi che il messaggio debba effettivamente essere classificato come spam.





La finestra di dialogo **Impostazioni delle prestazioni del motore** (accessibile dalla voce **Prestazioni** del menu di esplorazione a sinistra) include le impostazioni delle prestazioni del componente **Anti-Spam**:

Spostare il dispositivo di scorrimento a sinistra o a destra per modificare il livello dell'intervallo delle prestazioni di scansione tra le modalità **Desktop low-end/Desktop high-end**.

- **Desktop low-end** - durante il processo di scansione per l'identificazione dello spam non viene utilizzata alcuna regola. Per l'identificazione dello spam verranno utilizzati solo i dati di formazione. Questa modalità non è consigliata, a meno che l'hardware del computer non sia estremamente limitato.
- **Desktop high-end** - questa modalità richiederà una notevole quantità di memoria. Durante il processo di scansione per l'identificazione dello spam verranno utilizzate le seguenti funzionalità: regole e cache del database di spam, regole di base e avanzate, indirizzi IP e database di spammer.

La voce **Abilita controllo online** è attiva per impostazione predefinita. Ne risulta un rilevamento dello spam più preciso tramite la comunicazione con i server [Mailshell](#), ovvero i dati sottoposti a scansione verranno confrontati con i database [Mailshell](#) online.

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

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

Nell'interfaccia di modifica è possibile compilare un elenco di mittenti da cui si ha la certezza che non verranno mai inviati messaggi indesiderati (spam). È inoltre possibile compilare un elenco di nomi di dominio completi (ad esempio *avg.com*) che non generano mai messaggi spam. Dopo che è stato preparato un simile elenco di mittenti e/o nomi di dominio, è possibile inserirli in due modi diversi: inserendo direttamente ciascun indirizzo email o importando tutto l'elenco di indirizzi.

### **Pulsanti di controllo**

Sono disponibili i seguenti pulsanti di controllo:

- **Modifica** - selezionare questo pulsante per aprire una finestra di dialogo in cui è possibile immettere manualmente un elenco di indirizzi (è inoltre possibile utilizzare il metodo copia e incolla). Immettere una voce (mittente o nome di dominio) per riga.
- **Esporta** - se per qualsiasi motivo si decide di esportare i record, è possibile fare clic sul pulsante per eseguire l'operazione. Tutti i record verranno salvati in un file di testo normale.
- **Importa** - se si possiede già un file di testo di indirizzi di posta elettronica o nomi di dominio, è possibile importare tale file selezionando questo pulsante. Il file deve includere una sola voce (indirizzo, nome di dominio) per riga.





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

Nell'interfaccia di modifica è possibile compilare un elenco di mittenti da cui si ha la certezza di ricevere messaggi indesiderati (*spam*). È inoltre possibile compilare un elenco di nomi di dominio completi (*ad esempio aziendaspam.com*) da cui si prevede di ricevere o si ricevono messaggi di spam. Tutti i messaggi di posta elettronica ricevuti da tali indirizzi o domini specifici verranno contrassegnati come spam. Dopo che è stato preparato un simile elenco di mittenti e/o nomi di dominio, è possibile inserirli in due modi diversi: inserendo direttamente ciascun indirizzo email o importando tutto l'elenco di indirizzi.

### **Pulsanti di controllo**

Sono disponibili i seguenti pulsanti di controllo:

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

***Il ramo Impostazioni avanzate contiene opzioni di impostazione complete per la funzione Anti-Spam. Queste impostazioni sono destinate esclusivamente agli utenti esperti, in particolare agli amministratori di rete che devono eseguire una configurazione dettagliata della protezione anti-spam per garantire la massima protezione dei server email. Per questo motivo non è disponibile una guida aggiuntiva nelle singole finestre di dialogo. Tuttavia, è disponibile direttamente nell'interfaccia utente una breve descrizione di ciascuna opzione. Si consiglia di non modificare alcuna impostazione a meno che non si abbiano familiarità con tutte le impostazioni avanzate di Spamcatcher (MailShell Inc.). Eventuali modifiche inappropriate possono dare luogo a una riduzione delle prestazioni o a un funzionamento errato del componente.***

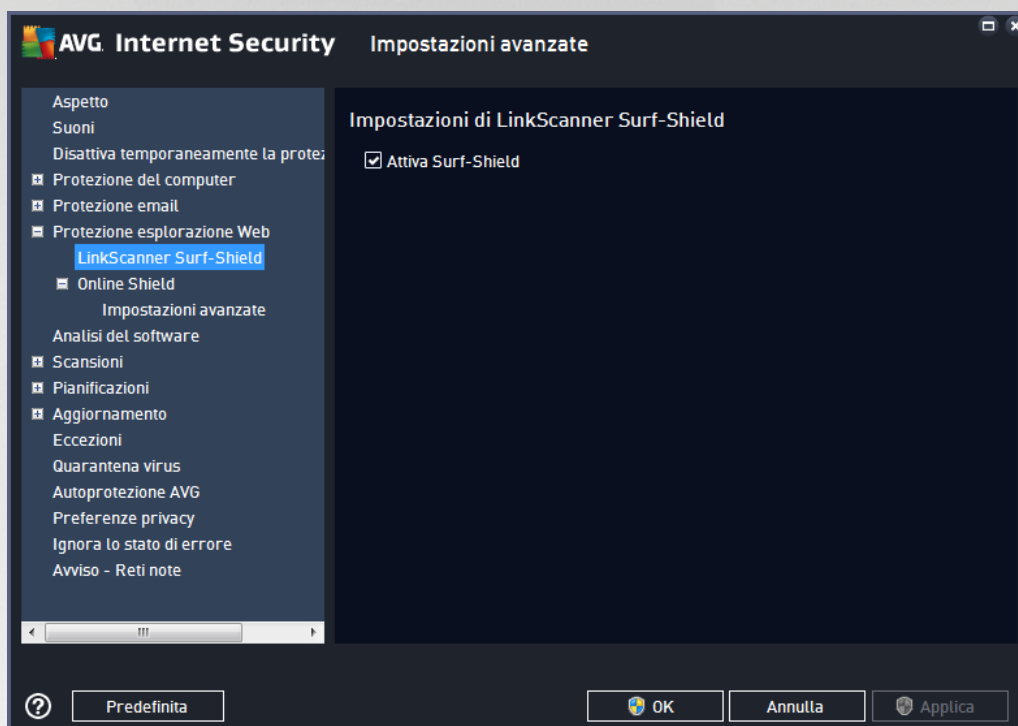
Se si ritiene di dover modificare comunque la configurazione Anti-Spam a un livello molto avanzato, seguire le istruzioni fornite direttamente nell'interfaccia utente. In genere, in ciascuna finestra di dialogo è contenuta una sola funzionalità specifica che può essere modificata. La relativa descrizione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

- **Filtraggio**: elenco lingue, elenco paesi, IP approvati, IP bloccati, paesi bloccati, set di caratteri bloccati, mittenti contraffatti
- **RBL**: server RBL, multihit, soglia, timeout, IP massimi
- **Connessione Internet**: timeout, server proxy, autenticazione proxy



### 3.5.6. Protezione esplorazione Web

La finestra di dialogo *Impostazioni LinkScanner* consente di attivare/disattivare le seguenti funzioni:

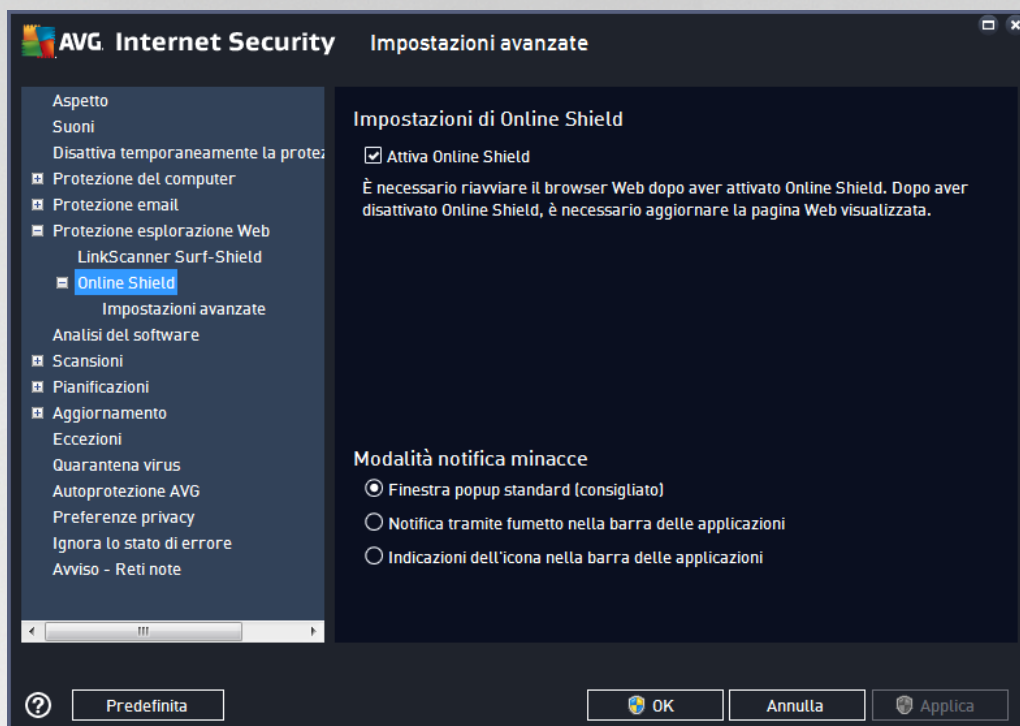


- **Abilita Surf-Shield** - (attivata per impostazione predefinita): protezione attiva, *in tempo reale*, da siti dannosi al momento dell'accesso. Le connessioni a siti dannosi noti e il relativo contenuto vengono bloccati non appena l'utente esegue l'accesso mediante un browser Web (o qualsiasi altra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



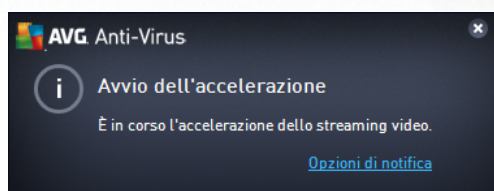


### 3.5.6.1. Online Shield



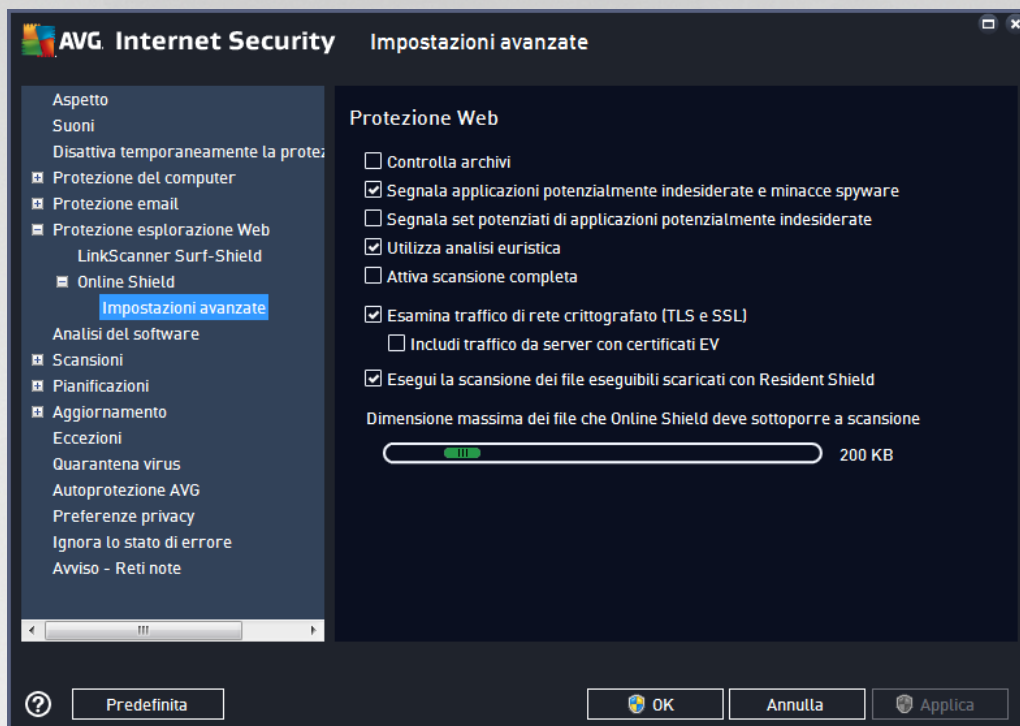
La finestra di dialogo **Online Shield** presenta le seguenti opzioni:

- **Abilita Online Shield** (attivata per impostazione predefinita) - attiva/disattiva l'intero servizio **Online Shield**. Per informazioni su altre impostazioni avanzate di **Online Shield**, passare alla successiva finestra di dialogo denominata [Protezione Web](#).
- **Attiva AVG Accelerator** (attivata per impostazione predefinita) - consente di attivare/disattivare il servizio AVG Accelerator. AVG Accelerator ottimizza la riproduzione dei video online e semplifica il download. Quando il processo di accelerazione video è in corso, l'utente ne verrà informato tramite la finestra a comparsa nell'area di notifica.



#### Modalità notifica minacce

Nella parte inferiore della finestra di dialogo, scegliere in che modo si desidera essere informati circa eventuali minacce rilevate: mediante una normale finestra a comparsa oppure mediante una notifica a fumetto o un'icona nell'area di notifica della barra delle applicazioni.



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

- **Controlla archivi** (*disattivata per impostazione predefinita*): consente di eseguire la scansione del contenuto di eventuali archivi inclusi nella pagina Web da visualizzare.
- **Segnala applicazioni potenzialmente indesiderate e minacce spyware** (*attivata per impostazione predefinita*): selezionare questa casella di controllo per attivare la scansione per ricercare spyware e virus. Gli spyware rappresentano una categoria di malware anomala: anche se solitamente costituiscono un rischio per la sicurezza, alcuni di questi programmi possono essere installati intenzionalmente. Si consiglia di mantenere questa funzionalità attivata in quanto consente di aumentare la protezione del computer.
- **Segnala set potenziati di applicazioni potenzialmente indesiderate** - (*disattivata per impostazione predefinita*): selezionare questa casella di controllo per rilevare pacchetti estesi di spyware, ovvero programmi perfettamente normali e innocui al momento dell'acquisto diretto presso il produttore, ma utilizzabili a scopi dannosi successivamente. Si tratta di una precauzione aggiuntiva che aumenta ulteriormente la protezione del computer, ma che potrebbe bloccare programmi legittimi, pertanto l'opzione è disattivata per impostazione predefinita.
- **Usa analisi euristiche** (*attivata per impostazione predefinita*): consente di eseguire la scansione del contenuto della pagina da visualizzare utilizzando il metodo dell'analisi euristica (*emulazione dinamica delle istruzioni dell'oggetto sottoposto a scansione in un ambiente informatico virtuale*).
- **Attiva scansione completa** (*disattivata per impostazione predefinita*): in situazioni specifiche





(se si sospetta che il computer sia stato infettato) per maggiore sicurezza è possibile selezionare questa opzione per attivare gli algoritmi di scansione più completi che esamineranno anche le aree del computer che difficilmente vengono infettate. Tenere presente tuttavia che questo metodo è piuttosto dispendioso in termini di tempo.

- **Esamina traffico di rete crittografato (TLS e SSL)** (attivata per impostazione predefinita): lasciare l'opzione selezionata per consentire ad AVG di analizzare anche le comunicazioni di rete crittografate, ovvero le connessioni tramite protocolli di sicurezza (SSL e la relativa versione più recente, TLS). Questa opzione si applica ai siti Web che utilizzano HTTPS e alle connessioni client email tramite TLS/SSL. Il traffico protetto viene decrittografato, esaminato per individuare eventuali malware e crittografato nuovamente per essere recapitato in modo sicuro al computer. In questa opzione è possibile selezionare anche **Includi traffico da server con certificati EV**, per analizzare anche le comunicazioni di rete crittografate da server certificati con certificati di convalida estesa. L'emissione di un certificato EV richiede una convalida estesa da parte dell'autorità di certificazione, pertanto i siti Web che presentano tale certificato sono più affidabili (ovvero hanno minori probabilità di distribuire malware). Per questo motivo, è possibile decidere di non sottoporre a scansione il traffico proveniente dai server certificati EV e ottenere quindi comunicazioni crittografate più rapide.
- **Esegui scansione dei file eseguibili scaricati con Resident Shield** (attivata per impostazione predefinita): consente di eseguire la scansione dei file eseguibili (in genere con estensioni exe, bat, com) dopo il download. Resident Shield esegue la scansione dei file prima del download per assicurare che non venga introdotto nessun file dannoso nel computer. Tuttavia, questa scansione è limitata dalla **dimensione massima del file da sottoporre a scansione** (vedere l'elemento successivo nella finestra di dialogo). I file di dimensioni maggiori, pertanto, vengono sottoposti a scansione una parte per volta e ciò si applica anche alla maggior parte dei file eseguibili. I file eseguibili possono eseguire diverse attività nel computer, perciò è fondamentale che siano completamente sicuri. Quindi, per una maggiore sicurezza, oltre alla scansione delle singole parti prima del download è opportuno sottoporre a scansione il file anche dopo il download. È consigliabile mantenere quest'opzione selezionata. Se questa opzione non viene attivata, si ha comunque la certezza che AVG rileverà qualsiasi codice potenzialmente pericoloso. Tuttavia, in genere non è in grado di valutare un file eseguibile nel complesso, perciò potrebbe creare dei falsi positivi.

Il dispositivo di scorrimento disponibile nella parte inferiore della finestra di dialogo consente di impostare la **dimensione massima del file da esaminare**: se i file inclusi sono presenti nella pagina visualizzata è inoltre possibile eseguire la scansione del relativo contenuto prima che vengano scaricati nel computer. Tuttavia, la scansione di file di grandi dimensioni richiede parecchio tempo rallentando notevolmente il download della pagina Web. È possibile utilizzare il dispositivo di scorrimento per specificare la dimensione massima dei file che **Online Shield** deve ancora sottoporre a scansione. Anche se le dimensioni del file scaricato sono superiori a quelle specificate, e di conseguenza il file non verrà sottoposto a scansione da Online Shield, il computer è comunque protetto: se il file fosse infetto, verrebbe rilevato immediatamente da **Resident Shield**.

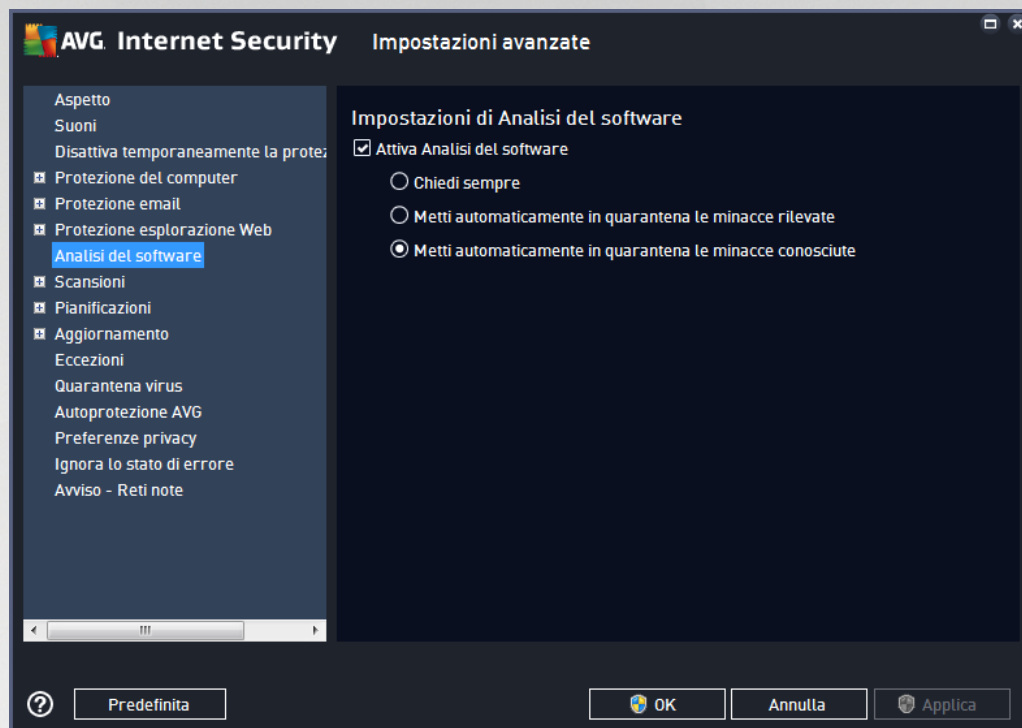
### 3.5.7. Analisi del software

**Analisi del software** è un componente anti-malware che protegge il computer da qualsiasi tipo di malware (spyware, bot, furti di identità e così via) utilizzando tecnologie basate sul comportamento e fornisce la protezione zero day per i nuovi virus (per una descrizione dettagliata delle funzionalità del componente, vedere il capitolo [Analisi del software](#)).

La finestra di dialogo **Impostazioni di Analisi del software** consente di attivare/disattivare le funzioni di base



del componente [Analisi del software](#):



**Attiva Analisi del software** (attivata per impostazione predefinita) - deselezionare questa casella di controllo per disattivare il componente [Identità](#). **Si consiglia di non disattivare questo componente a meno che non sia assolutamente necessario.** Quando Analisi del software è attivato, è possibile specificare l'azione da intraprendere quando viene rilevata una minaccia:

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

### 3.5.8. Scansioni

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

- [Scansione intero computer](#): scansione predefinita standard dell'intero computer
- [Scansione file o cartelle](#): scansione predefinita standard di aree selezionate del computer
- [Scansione estensione shell](#): scansione specifica di un oggetto selezionato direttamente dall'ambiente Esplora risorse

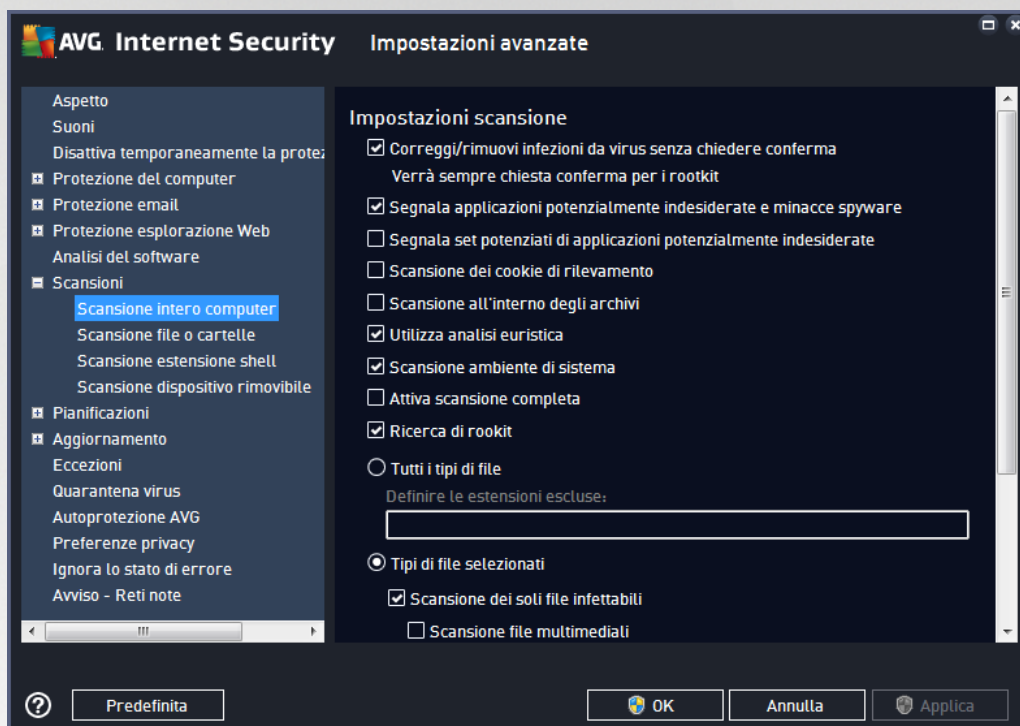




- [Scansione dispositivo rimovibile](#): scansione specifica di dispositivi rimovibili collegati al computer

### 3.5.8.1. Scansione intero computer

L'opzione **Scansione intero computer** consente di modificare i parametri di una delle scansioni predefinite dal fornitore del software, ossia [Scansione intero computer](#):



#### Impostazioni scansione

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

- **Correggi/Rimuovi infezioni da virus senza richiedere conferma** (attivata per impostazione predefinita): se viene identificato un virus durante la scansione, può essere corretto automaticamente se è disponibile una soluzione. Se il file infetto non può essere corretto automaticamente, l'oggetto infetto verrà spostato in [Quarantena virus](#).
- **Segnala applicazioni potenzialmente indesiderate e minacce spyware** (attivata per impostazione predefinita): selezionare questa casella di controllo per attivare la scansione per ricercare spyware e virus. Gli spyware rappresentano una categoria di malware anomala: anche se solitamente costituiscono un rischio per la sicurezza, alcuni di questi programmi possono essere installati intenzionalmente. Si consiglia di mantenere questa funzionalità attivata in quanto consente di aumentare la protezione del computer.
- **Segnala set potenziati di applicazioni potenzialmente indesiderate** (disattivata per impostazione predefinita): selezionare per rilevare pacchetti estesi di spyware, ovvero programmi perfettamente normali e innocui al momento dell'acquisto diretto presso il produttore, ma utilizzabili a scopi dannosi successivamente. Si tratta di una precauzione aggiuntiva che aumenta ulteriormente la protezione del computer, ma che potrebbe bloccare programmi legittimi, pertanto l'opzione è disattivata per



impostazione predefinita.

- **Scansione dei cookie di rilevamento** (disattivata per impostazione predefinita): questo parametro specifica che i cookie devono essere rilevati; (i cookie HTTP vengono utilizzati per autenticare, rilevare e mantenere informazioni specifiche sugli utenti, quali le preferenze dei siti o il contenuto dei carrelli elettronici).
- **Scansione all'interno degli archivi** (disattivata per impostazione predefinita): questo parametro specifica che la scansione deve controllare tutti i file inclusi all'interno di un archivio, quali ZIP, RAR e così via.
- **Usa analisi euristiche** (attivata per impostazione predefinita): l'analisi euristica (emulazione dinamica della istruzioni dell'oggetto sottoposto a scansione in un ambiente informatico virtuale) sarà uno dei metodi utilizzati per il rilevamento di virus durante la scansione.
- **Scansione ambiente di sistema** (attivata per impostazione predefinita): la scansione verrà eseguita anche sulle aree di sistema del computer.
- **Attiva scansione completa** (disattivata per impostazione predefinita): in situazioni specifiche (se si sospetta che il computer sia stato infettato) per maggiore sicurezza è possibile selezionare questa opzione per attivare gli algoritmi di scansione più completi che esamineranno anche le aree del computer che difficilmente vengono infettate. Tenere presente tuttavia che questo metodo è piuttosto dispendioso in termini di tempo.
- **Ricerca di rootkit** (attivata per impostazione predefinita): la scansione [Anti-Rootkit](#) cerca nel PC possibili rootkit, ovvero programmi e tecnologie che possono coprire l'attività dei malware nel computer. Se viene rilevato un rootkit, ciò non significa necessariamente che il computer sia infetto. In alcuni casi, specifici driver o sezioni di applicazioni regolari possono venire rilevati erroneamente come rootkit.

Inoltre, è necessario decidere quali elementi sottoporre a scansione

- **Tutti i tipi di file** con l'opzione per definire le eccezioni fornendo un elenco di estensioni di file separate da virgola da non sottoporre a scansione (dopo il salvataggio, le virgole vengono sostituite da punto e virgola).
- **Tipi di file selezionati**: è possibile specificare che si desidera sottoporre a scansione solo i file potenzialmente infettabili (i file che non possono essere infettati non verranno sottoposti a scansione, ad esempio alcuni file di testo normale o altri file non eseguibili), inclusi i file multimediali (file video e audio; se non si seleziona questa casella, il tempo di scansione risulterà ulteriormente ridotto, poiché questi file sono spesso di grandi dimensioni e non facilmente infettabili dai virus). Anche in questo caso, è possibile specificare tramite le estensioni quali file devono essere sempre sottoposti a scansione.
- Facoltativamente, è possibile effettuare la **Scansione dei file senza estensioni**: questa opzione è attivata per impostazione predefinita e si consiglia di non modificarla a meno che non si abbiano motivi validi per farlo. I file senza estensione sono piuttosto sospetti e devono essere sempre sottoposti a scansione.

### Regola la velocità di completamento della scansione

All'interno della sezione **Regola la velocità di completamento della scansione** è inoltre possibile specificare

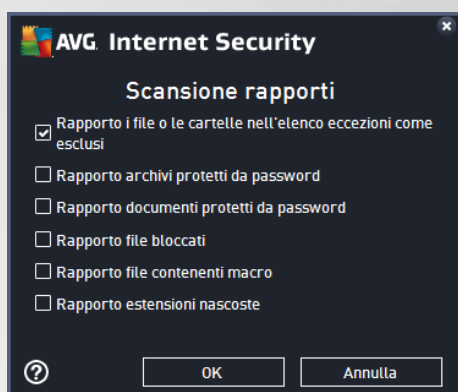




la velocità di scansione desiderata in base all'utilizzo delle risorse di sistema. Per impostazione predefinita, questa opzione è impostata sul livello *sensibile all'utente* per l'utilizzo automatico delle risorse. Se si desidera aumentare la velocità della scansione, il tempo impiegato sarà inferiore ma l'utilizzo delle risorse di sistema aumenterà notevolmente durante l'esecuzione e rallenterà le altre attività svolte sul PC (*questa opzione può essere utilizzata quando il computer è acceso ma non in uso*). Tuttavia, è possibile diminuire l'utilizzo delle risorse di sistema aumentando la durata della scansione.

### **Imposta rapporti di scansione aggiuntivi...**

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



### **3.5.8.2. Scansione file o cartelle**

L'interfaccia di modifica di **Scansione file o cartelle** è quasi identica alla finestra di dialogo di modifica di [Scansione intero computer](#), tuttavia le impostazioni predefinite sono più restrittive per [Scansione intero computer](#):



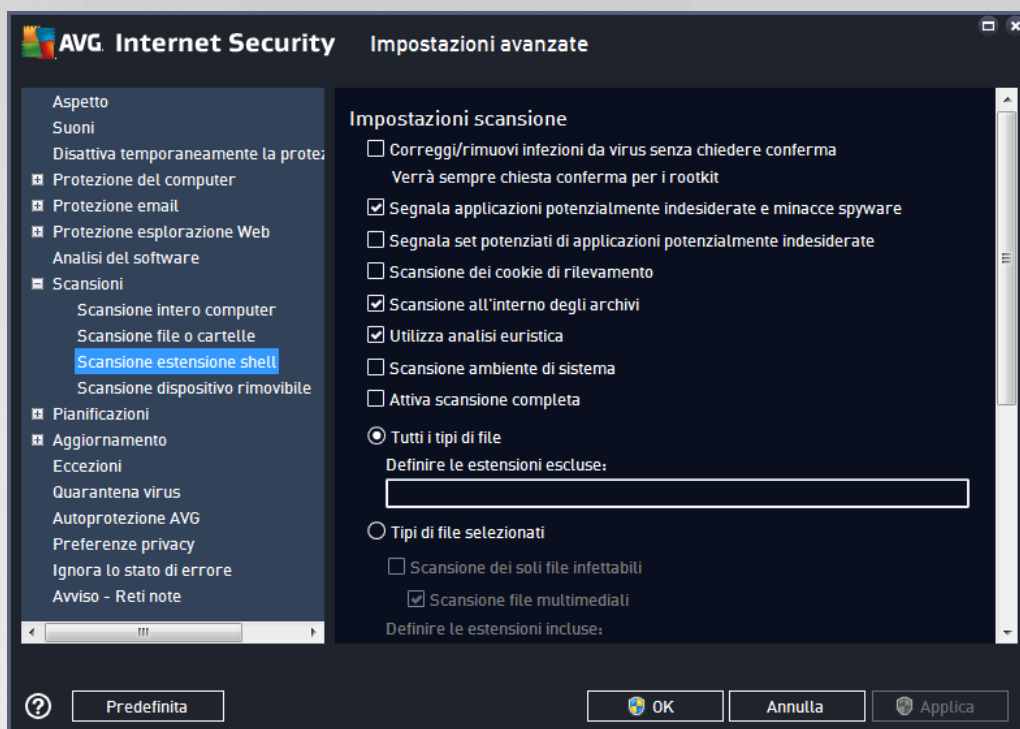
Tutti i parametri impostati in questa finestra di dialogo di configurazione si applicano solo alle aree selezionate per la scansione con [Scansione file o cartelle](#).

**Nota:** per una descrizione dei parametri specifici, vedere il capitolo [Impostazioni avanzate di AVG / Scansione / Scansione intero computer](#).

### 3.5.8.3. Scansione estensione shell

Analogamente a [Scansione intero computer](#), **Scansione estensione shell** offre diverse opzioni per modificare la scansione predefinita dal fornitore del software. In questo caso, la configurazione è correlata alla [scansione di oggetti specifici avviata direttamente dall'ambiente Esplora risorse](#) (estensione shell), vedere il capitolo [Scansione in Esplora risorse](#):





Le opzioni di modifica sono quasi identiche a quelle disponibili per [Scansione intero computer](#), tuttavia, le impostazioni predefinite sono diverse (*ad esempio, per impostazione predefinita, Scansione intero computer non controlla gli archivi ma esegue la scansione dell'ambiente di sistema e viceversa per Scansione estensione shell*).

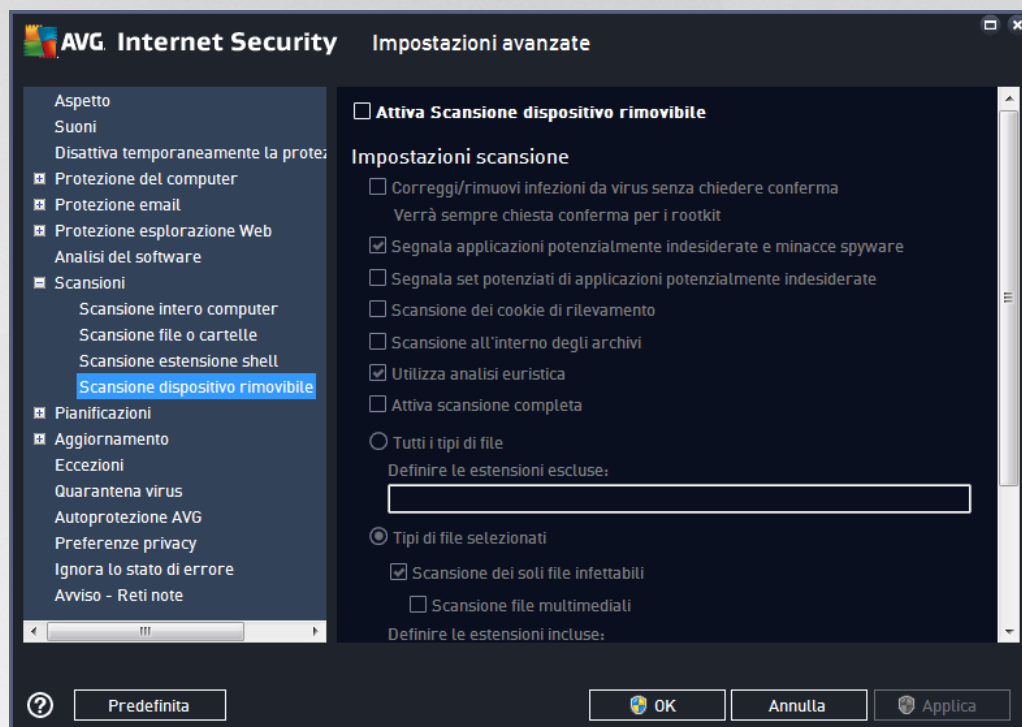
**Nota:** per una descrizione dei parametri specifici, vedere il capitolo [Impostazioni avanzate di AVG / Scansione / Scansione intero computer](#).

Rispetto alla finestra di dialogo [Scansione intero computer](#), la finestra di dialogo **Scansione estensione shell** include anche la sezione denominata **Visualizzazione dei risultati e dell'avanzamento della scansione**, in cui è possibile specificare se si desidera accedere all'avanzamento della scansione e ai risultati della scansione dall'interfaccia utente di AVG. Inoltre, è possibile definire se il risultato della scansione deve essere visualizzato solo nel caso in cui venga rilevata un'infezione durante la scansione.



### 3.5.8.4. Scansione dispositivo rimovibile

Anche l'interfaccia di modifica di **Scansione dispositivo rimovibile** è molto simile alla finestra di dialogo di modifica di [Scansione intero computer](#):



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

**Nota:** per una descrizione dei parametri specifici, vedere il capitolo [Impostazioni avanzate di AVG / Scansione / Scansione intero computer](#).

### 3.5.9. Pianificazioni

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

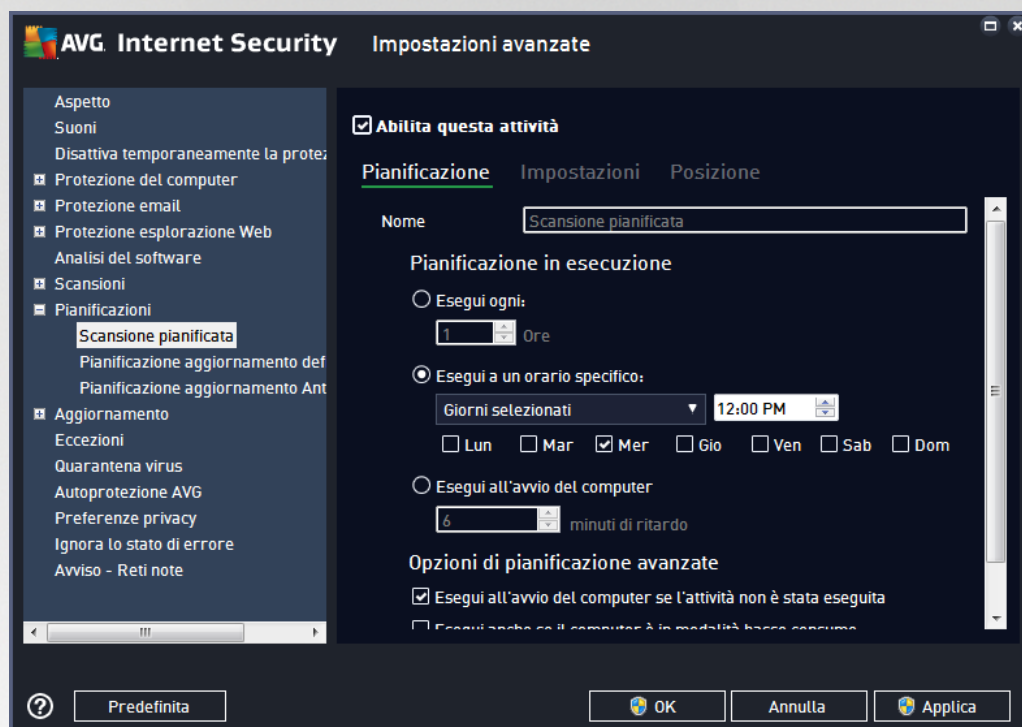
- [Scansione pianificata](#)
- [Pianificazione aggiornamento definizioni](#)
- Pianificazione dell'aggiornamento del programma
- [Pianificazione aggiornamenti Anti-Spam](#)





### 3.5.9.1. Scansione pianificata

È possibile modificare i parametri della scansione pianificata (o impostare una nuova pianificazione) in tre schede. In ciascuna scheda è possibile selezionare/deselezionare la voce **Abilita questa attività** per disattivare temporaneamente il controllo pianificato e riattivarlo secondo le necessità:



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

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

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

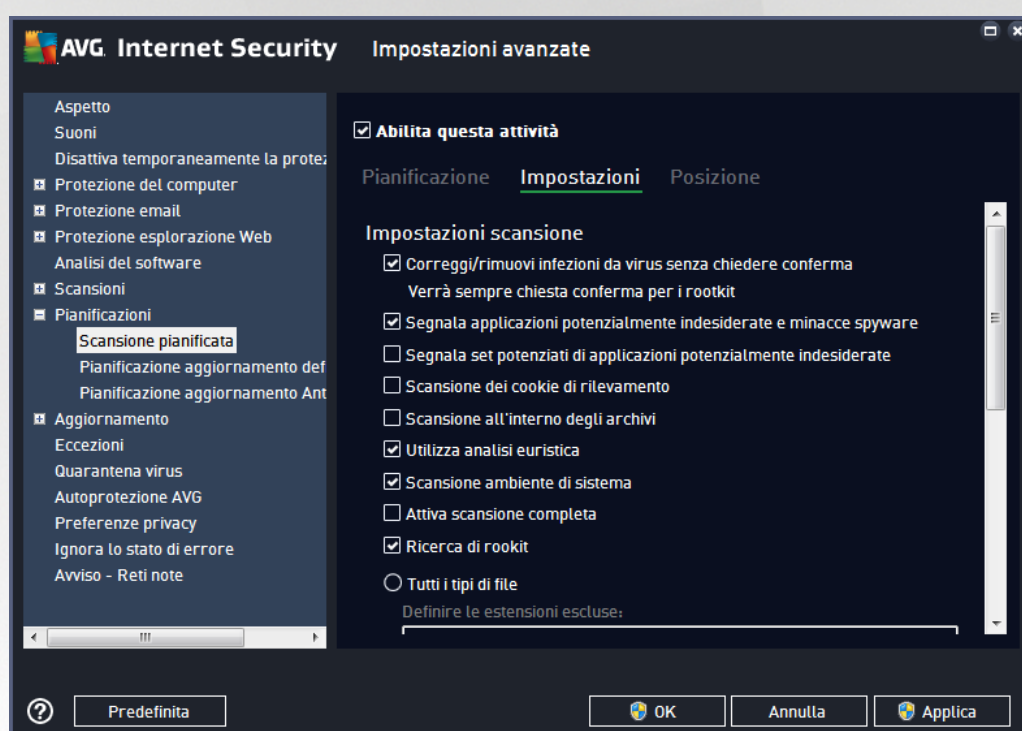
#### Pianificazione in esecuzione

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



## Opzioni di pianificazione avanzate

- **Esegui all'avvio del computer se l'attività non è stata eseguita** - se si pianifica l'esecuzione dell'attività a un'ora specifica, questa opzione consentirà di verificare che la scansione venga eseguita in un momento successivo nel caso in cui il computer sia spento all'ora della pianificazione.
- **Esegui anche se il computer è in modalità basso consumo** - consente di specificare se la scansione deve essere eseguita anche se il computer è in esecuzione con alimentazione a batteria all'orario pianificato.



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

- **Correggi/Rimuovi infezioni da virus senza richiedere conferma** (attivata per impostazione predefinita): se viene identificato un virus durante la scansione può essere corretto automaticamente se è disponibile una soluzione. Se il file infetto non può essere corretto automaticamente, l'oggetto infetto verrà spostato in [Quarantena virus](#).
- **Segnala applicazioni potenzialmente indesiderate e minacce spyware** (attivata per impostazione predefinita): selezionare questa casella di controllo per attivare la scansione per ricercare spyware e virus. Gli spyware rappresentano una categoria di malware anomala: anche se solitamente costituiscono un rischio per la sicurezza, alcuni di questi programmi possono essere installati intenzionalmente. Si consiglia di mantenere questa funzionalità attivata in quanto consente di aumentare la protezione del computer.
- **Segnala set potenziati di applicazioni potenzialmente indesiderate** (disattivata per impostazione





*predefinita*): selezionare per rilevare pacchetti estesi di spyware, ovvero programmi perfettamente normali e innocui al momento dell'acquisto diretto presso il produttore, ma utilizzabili a scopi dannosi successivamente. Si tratta di una precauzione aggiuntiva che aumenta ulteriormente la protezione del computer, ma che potrebbe bloccare programmi legittimi, pertanto l'opzione è disattivata per impostazione predefinita.

- **Scansione dei cookie di rilevamento** (*disattivata per impostazione predefinita*): questo parametro stabilisce che i cookie devono essere rilevati durante la scansione (*i cookie HTTP vengono utilizzati per autenticare, rilevare e mantenere informazioni specifiche sugli utenti, quali i siti preferiti o il contenuto dei carrelli elettronici*).
- **Scansione all'interno degli archivi** (*disattivata per impostazione predefinita*): questo parametro stabilisce che la scansione deve controllare tutti i file anche se inclusi all'interno di un tipo di archivio, quale ZIP, RAR e così via.
- **Usa analisi euristiche** (*attivata per impostazione predefinita*): l'analisi euristica (*emulazione dinamica delle istruzioni dell'oggetto sottoposto a scansione in un ambiente informatico virtuale*) sarà uno dei metodi utilizzati per il rilevamento di virus durante la scansione.
- **Scansione ambiente di sistema** (*attivata per impostazione predefinita*): la scansione verrà eseguita anche sulle aree di sistema del computer.
- **Attiva scansione completa** (*disattivata per impostazione predefinita*): in situazioni specifiche (*ad esempio se si sospetta che il computer sia stato infettato*) per maggiore sicurezza è possibile selezionare questa opzione per attivare gli algoritmi di scansione più completi che esamineranno anche le aree del computer che difficilmente vengono infettate. Tenere presente tuttavia che questo metodo è piuttosto dispendioso in termini di tempo.
- **Ricerca di rootkit** (*attivata per impostazione predefinita*): la scansione Anti-Rootkit ricerca sul computer la presenza di eventuali rootkit (programmi e tecnologie in grado di coprire l'attività dei malware nel computer). Se viene rilevato un rootkit, ciò non significa necessariamente che il computer sia infetto. In alcuni casi, specifici driver o sezioni di applicazioni regolari possono venire rilevati erroneamente come rootkit.

Inoltre, è necessario decidere quali elementi sottoporre a scansione

- **Tutti i tipi di file** con l'opzione per definire le eccezioni fornendo un elenco di estensioni di file separate da virgola da non sottoporre a scansione (*dopo il salvataggio, le virgole vengono sostituite da punto e virgola*).
- **Tipi di file selezionati**: è possibile specificare che si desidera sottoporre a scansione solo i file potenzialmente infettabili (*i file che non possono essere infettati non verranno sottoposti a scansione, ad esempio alcuni file di testo normale o altri file non eseguibili*), inclusi i file multimediali (*file video e audio; se non si seleziona questa casella, il tempo di scansione risulterà ulteriormente ridotto, poiché questi file sono spesso di grandi dimensioni e non facilmente infettabili dai virus*). Anche in questo caso, è possibile specificare tramite le estensioni quali file devono essere sempre sottoposti a scansione.
- Facoltativamente, è possibile effettuare la **Scansione dei file senza estensioni**: questa opzione è attivata per impostazione predefinita e si consiglia di non modificarla a meno che non si abbiano motivi validi per farlo. I file senza estensione sono piuttosto sospetti e devono essere sempre sottoposti a scansione.



### Regola la velocità di completamento della scansione

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

### Imposta rapporti di scansione aggiuntivi

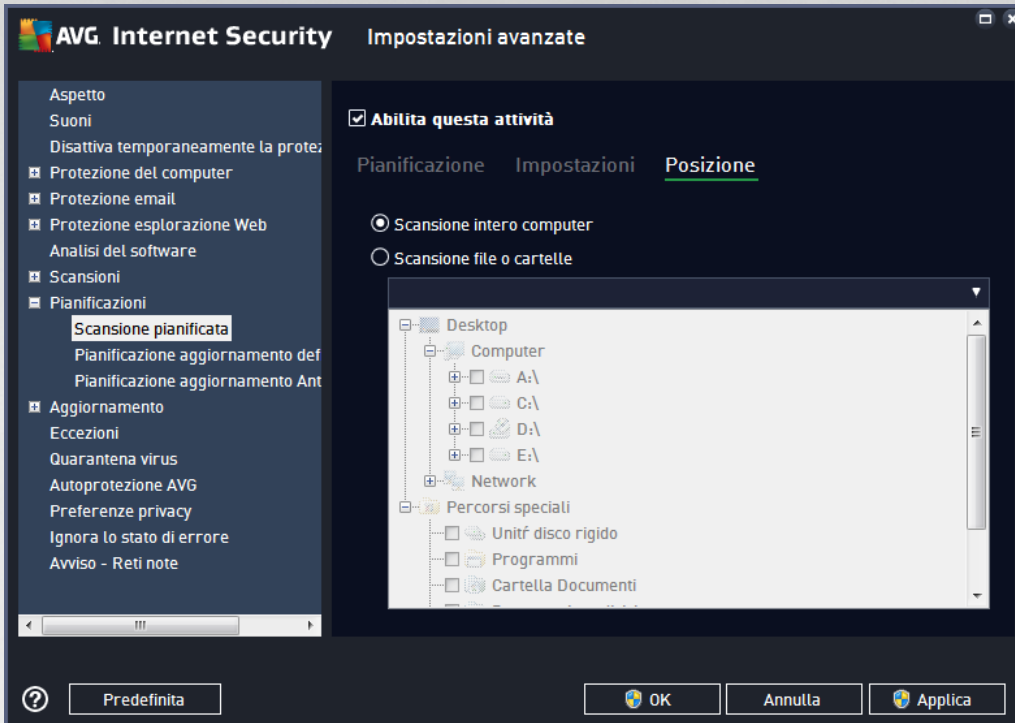
Fare clic sul collegamento *Imposta rapporti di scansione aggiuntivi...* per aprire una finestra di dialogo autonoma denominata *Rapporti di scansione* in cui è possibile selezionare diversi elementi per definire i tipi di rilevamenti da segnalare:



### Opzioni arresto computer

Nella sezione *Opzioni arresto computer*, è possibile decidere se il computer deve essere arrestato in modo automatico al termine del processo di scansione. Dopo aver confermato questa opzione (*Arresta computer al completamento della scansione*), viene attivata una nuova opzione che consente l'arresto del computer anche se è correntemente bloccato (*Forza arresto se il computer è bloccato*).



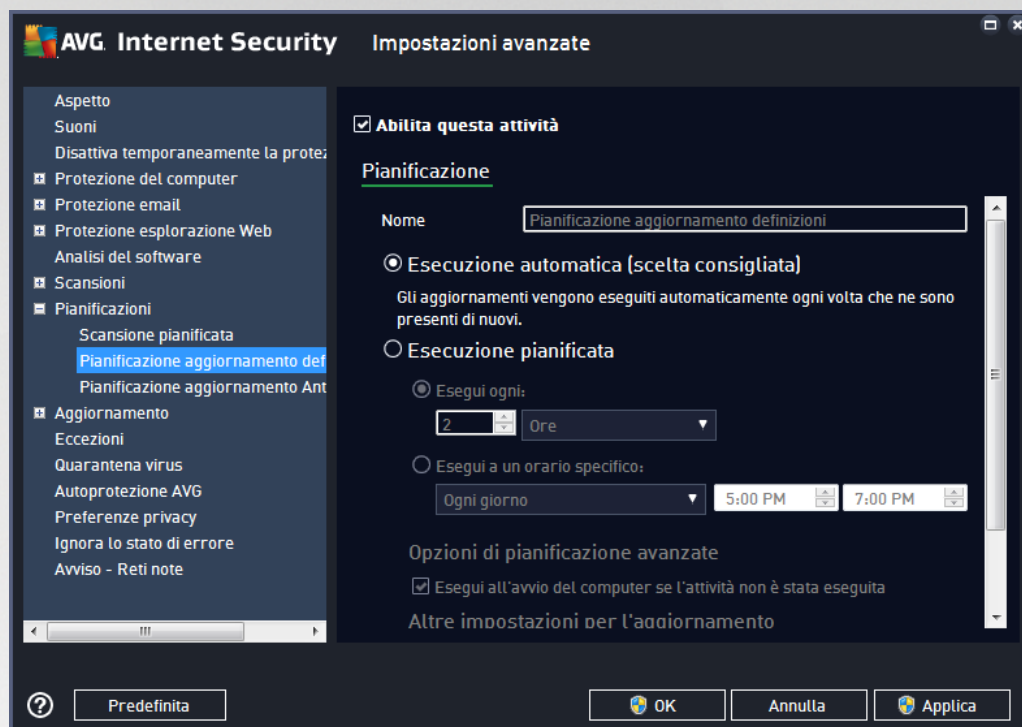


Nella scheda **Posizione** è possibile definire se si desidera pianificare la [scansione dell'intero computer](#) o la [scansione di file o cartelle](#). Se si seleziona la scansione di file o cartelle, nella parte inferiore di questa finestra di dialogo viene attivata la struttura visualizzata che consente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



### 3.5.9.2. Pianificazione aggiornamento definizioni

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



In questa finestra di dialogo è possibile impostare alcuni parametri dettagliati della pianificazione dell'aggiornamento delle definizioni. Nel campo di testo **Nome** (*disattivato per tutte le pianificazioni predefinite*) è presente il nome assegnato alla pianificazione in oggetto dal fornitore del programma.

#### Pianificazione in esecuzione

Per impostazione predefinita, l'attività viene avviata in modo automatico (**Esegui automaticamente**) non appena è disponibile un nuovo aggiornamento delle definizioni dei virus. Si consiglia di non modificare questa configurazione, a meno che non sia assolutamente necessario. È inoltre possibile impostare l'esecuzione dell'attività manualmente, specificando gli intervalli di tempo per l'avvio del nuovo aggiornamento delle definizioni pianificato. È possibile definire l'ora tramite l'avvio ripetuto dell'aggiornamento dopo un certo periodo di tempo (**Esegui ogni...**) oppure definendo data e ora esatte (**Esegui a un orario specifico**).

#### Opzioni di pianificazione avanzate

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

#### Altre impostazioni di aggiornamento

Infine, selezionare l'opzione **Esegui nuovamente l'aggiornamento quando la connessione Internet sarà disponibile** per assicurarsi che, se la connessione Internet si interrompesse e il processo di aggiornamento non riuscisse, tale processo venga avviato di nuovo subito dopo il ripristino della connessione Internet. Quando la scansione pianificata viene avviata all'ora specificata, l'utente ne viene informato tramite una finestra popup





visualizzata sopra l'icona di AVG nell'area di notifica (a condizione che sia stata mantenuta la configurazione predefinita della finestra di dialogo [Impostazioni avanzate/Aspetto](#)).

### **3.5.9.3. Pianificazione aggiornamenti Anti-Spam**

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

In questa finestra di dialogo è possibile impostare alcuni parametri dettagliati per la pianificazione dell'aggiornamento. Il campo di testo **Nome** (*disattivato per tutte le pianificazioni predefinite*) indica il nome assegnato alla pianificazione in oggetto dal fornitore del programma.

#### **Pianificazione in esecuzione**

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

#### **Opzioni di pianificazione avanzate**

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

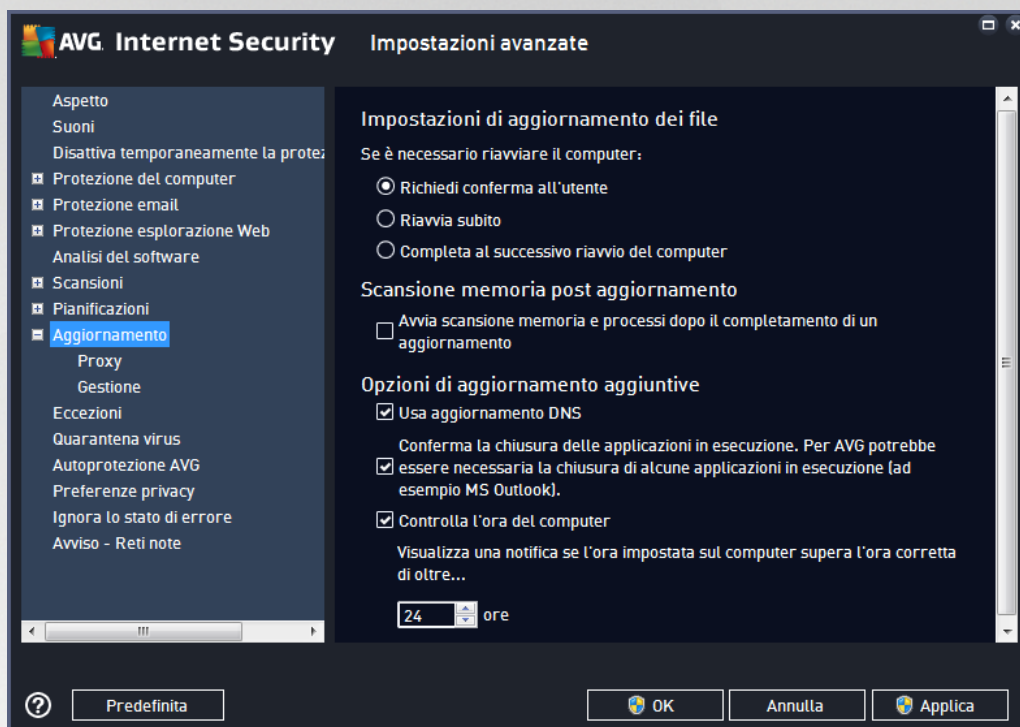
#### **Altre impostazioni di aggiornamento**

Selezionare l'opzione **Eseguire nuovamente l'aggiornamento quando la connessione Internet sarà disponibile** per assicurarsi che, se la connessione Internet si interrompesse e il processo di aggiornamento Anti-Spam non riuscisse, tale processo venga avviato di nuovo subito dopo il ripristino della connessione Internet. Quando la scansione pianificata viene avviata all'ora specificata, l'utente ne viene informato tramite una finestra popup visualizzata sopra l'icona di AVG nell'area di notifica (a condizione che sia stata mantenuta la configurazione predefinita della finestra di dialogo [Impostazioni avanzate/Aspetto](#)).



### 3.5.10. Aggiornamento

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



#### Quando eseguire l'aggiornamento dei file

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

- **Richiedi conferma dell'utente** (impostazione predefinita) - verrà richiesto di approvare un riavvio del PC necessario per finalizzare il processo di [aggiornamento](#)
- **Riavvia subito** - il computer verrà riavviato immediatamente in maniera automatica dopo la finalizzazione del processo di [aggiornamento](#) senza richiesta di conferma da parte dell'utente
- **Completa al successivo riavvio del computer** - la finalizzazione del processo di [aggiornamento](#) verrà posticipata al successivo riavvio del computer. Tenere presente che questa opzione è consigliata solo se si è certi che il computer venga riavviato regolarmente, almeno una volta al giorno.

#### Scansione memoria post aggiornamento

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

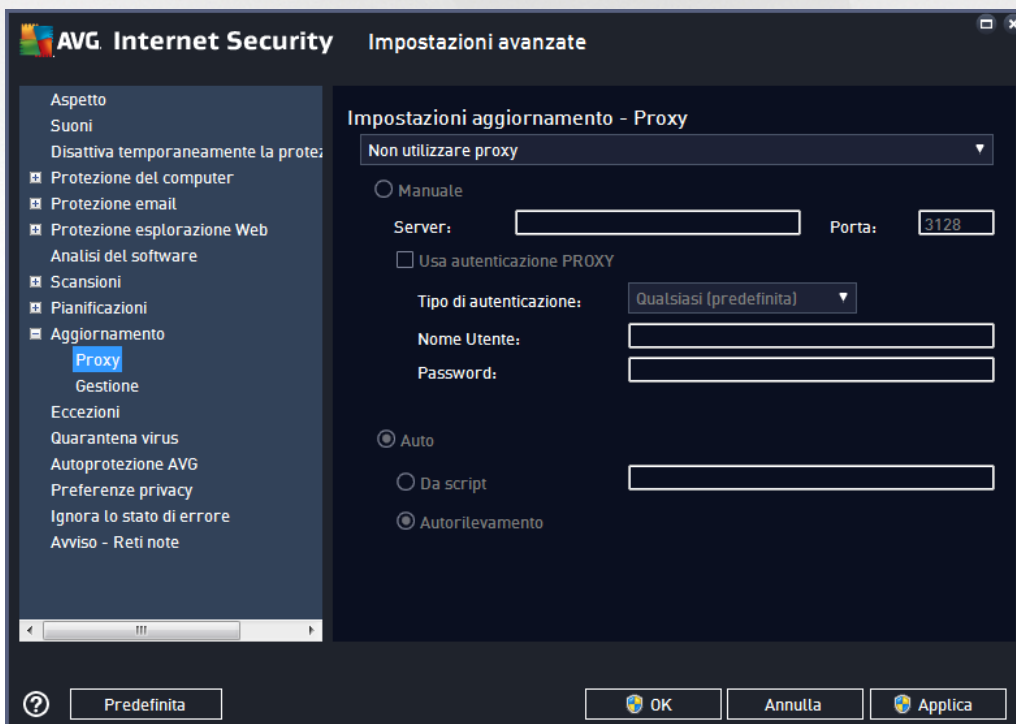




### Opzioni di aggiornamento aggiuntive

- **Crea nuovo punto di ripristino del sistema durante ogni aggiornamento del programma** (attivata per impostazione predefinita) - prima dell'avvio di ciascun aggiornamento del programma AVG viene creato un punto di ripristino del sistema. Se il processo di aggiornamento non ha esito positivo e il sistema operativo si blocca, è possibile ripristinare il sistema operativo nella configurazione originale da questo punto. Questa opzione è accessibile tramite Start / Tutti i programmi / Accessori / Utilità di sistema / Ripristino configurazione di sistema, tuttavia le eventuali modifiche sono consigliate ai soli utenti esperti. Mantenere selezionata questa casella di controllo se si desidera utilizzare questa funzionalità.
- **Usa aggiornamento DNS** (attivata per impostazione predefinita) - con questa voce selezionata, una volta avviato l'aggiornamento, **AVG Internet Security** ricerca informazioni sulla versione del database dei virus più recente e sulla versione del programma più recente sul server DNS. Quindi, solo i file di aggiornamento più piccoli e indispensabili vengono scaricati e applicati. In questo modo la quantità totale di dati scaricati viene ridotta al minimo e il processo di aggiornamento viene accelerato.
- **Conferma la chiusura delle applicazioni in esecuzione** (attivata per impostazione predefinita) - questa opzione garantirà che nessuna applicazione in esecuzione venga chiusa senza autorizzazione, nel caso fosse necessario per la finalizzazione del processo di aggiornamento.
- **Controlla l'ora del computer** (attivata per impostazione predefinita) - selezionare questa opzione per ricevere una notifica nel caso in cui l'ora del computer differisca dall'ora esatta di un valore superiore al numero di ore specificato.

### 3.5.10.1. Proxy



Il server proxy è un server autonomo o un servizio in esecuzione su un PC che garantisce una connessione più sicura a Internet. Secondo le regole di rete specificate è possibile accedere a Internet direttamente o tramite il



server proxy. Sono anche consentite entrambe le possibilità contemporaneamente. Quindi, nella prima voce della finestra di dialogo **Impostazioni aggiornamento - Proxy** è necessario selezionare l'opzione desiderata dal menu della casella combinata:

- **Non utilizzare proxy** - impostazione predefinita
- **Usa proxy**
- **Tenta la connessione utilizzando il proxy e, se non riesce, esegui la connessione direttamente**

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

### Configurazione manuale

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

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

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

### Configurazione automatica

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

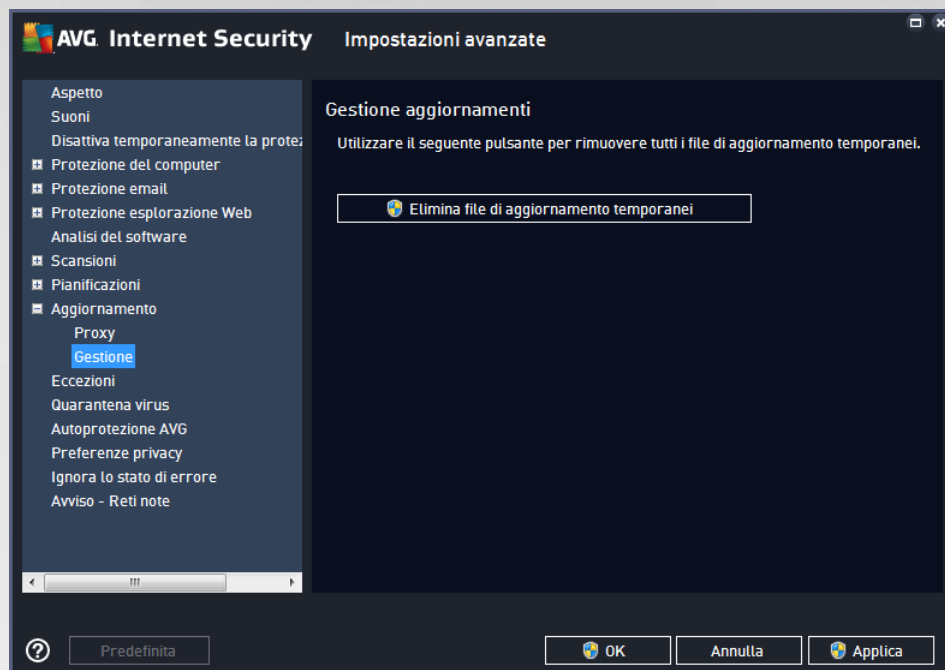
- **Da browser** - la configurazione verrà letta dal browser Internet predefinito
- **Da script** - la configurazione verrà letta da uno script scaricato con la funzione di restituzione dell'indirizzo proxy
- **Autorilevamento** - la configurazione verrà rilevata automaticamente direttamente dal server proxy





### 3.5.10.2. Gestione

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

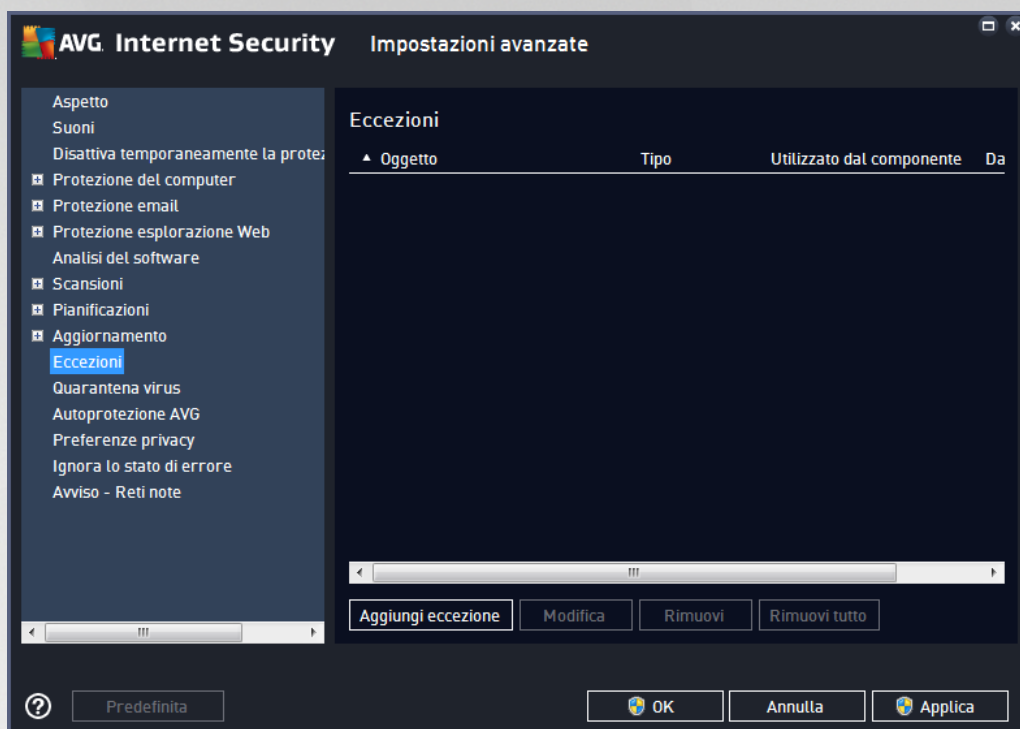


- **Elimina file di aggiornamento temporanei** - selezionare questo pulsante per eliminare tutti i file di aggiornamento ridondanti dal disco rigido (*per impostazione predefinita, questi file restano memorizzati per 30 giorni*)
- **Ripristina la precedente versione del database dei virus** - selezionare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

### 3.5.11. Eccezioni

Nella finestra di dialogo **Eccezioni** è possibile definire le eccezioni, ovvero voci che verranno ignorate da **AVG Internet Security**. In genere, sarà necessario definire un'eccezione se AVG continua a rilevare un programma o un file come se fosse una minaccia oppure blocca un sito Web sicuro come se fosse pericoloso. Se si aggiungono tali file o siti Web a questo elenco eccezioni, AVG non li segnalerà né bloccherà più.

**Assicurarsi sempre che il file, il programma o il sito Web in questione sia davvero completamente sicuro.**

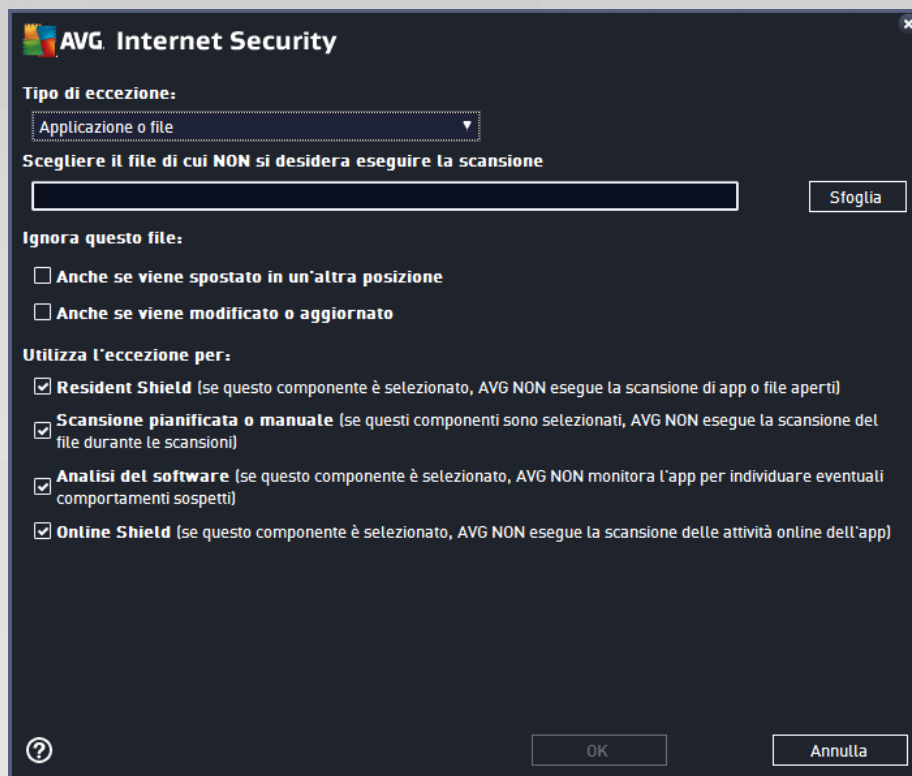


Nel grafico della finestra di dialogo viene visualizzato un elenco di eccezioni, se sono già state definite. Accanto a ogni elemento è presente una casella di controllo. Se la casella di controllo è selezionata, l'eccezione è attiva. In caso contrario, è semplicemente definita ma non utilizzata. Facendo clic su un'intestazione di colonna, è possibile ordinare gli elementi consentiti in base al criterio corrispondente.

### Pulsanti di controllo

- **Aggiungi eccezione:** fare clic per aprire una nuova finestra di dialogo in cui specificare la voce da escludere dalla scansione AVG.



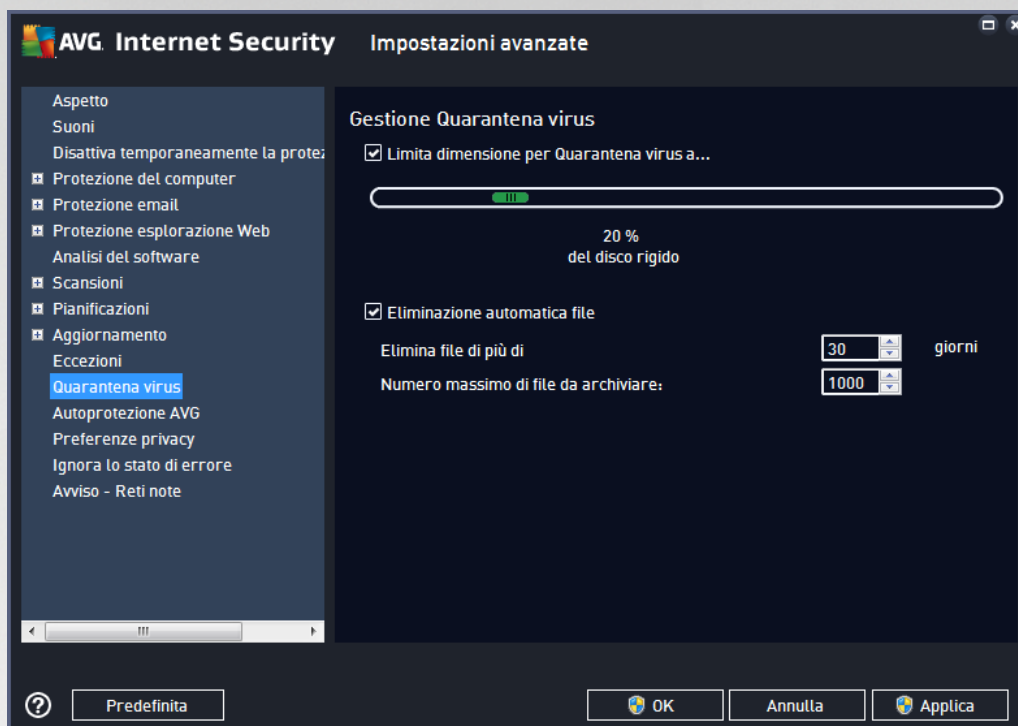


Prima di tutto, verrà richiesto di definire il tipo di oggetto, ovvero se si tratta di un'applicazione, un file, una cartella, un URL o un certificato. Quindi sarà necessario specificare il percorso del relativo oggetto nel disco o digitare l'URL. Infine, è possibile selezionare per quali funzionalità di AVG ignorare l'oggetto selezionato (*Resident Shield*, *Scansione pianificata o manuale*, *Analisi del software*, *Online Shield* e *Windows AMSI*).

- **Modifica:** questo pulsante è attivo solo se alcune eccezioni sono state già definite e inserite nell'elenco. È quindi possibile utilizzare il pulsante per aprire la finestra di modifica relativa all'eccezione selezionata e configurare i parametri dell'eccezione.
- **Rimuovi:** questo pulsante consente di annullare un'eccezione definita in precedenza. È possibile rimuovere le eccezioni una per una o evidenziare un blocco nell'elenco e annullare le eccezioni definite. Dopo aver annullato l'eccezione, il file, la cartella o l'URL relativi verranno controllati di nuovo da AVG. Tenere presente che verrà rimossa solo l'eccezione, non il relativo file o cartella.
- **Rimuovi tutte:** utilizzare questo pulsante per eliminare tutte le eccezioni definite nell'elenco.



### 3.5.12. Quarantena virus



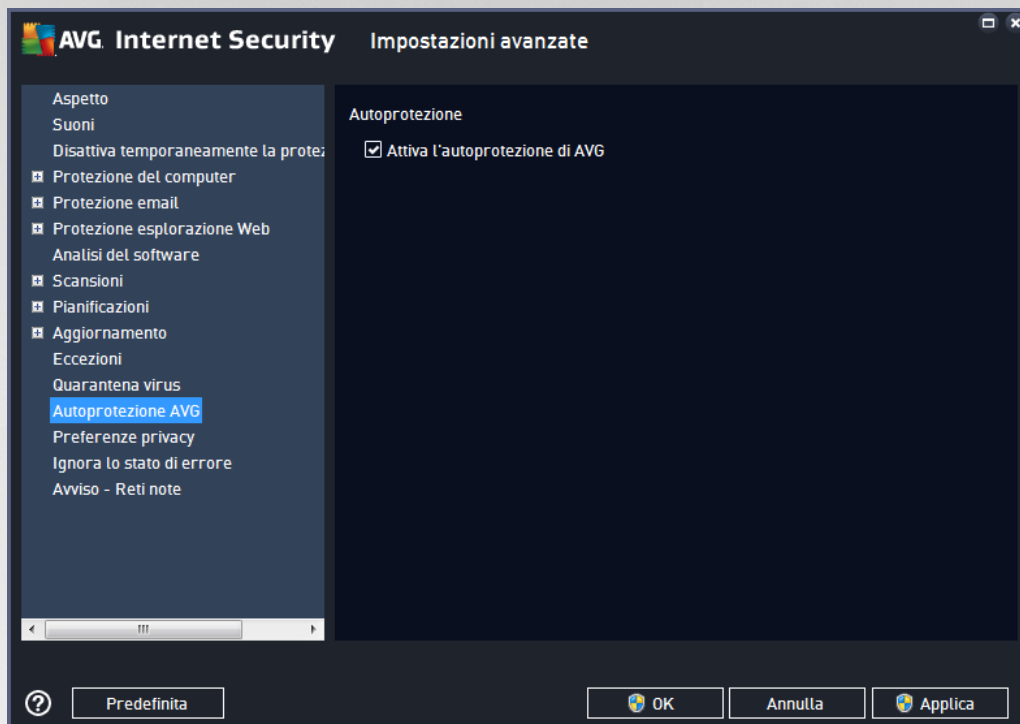
La finestra di dialogo **Gestione Quarantena virus** consente di definire diversi parametri relativi alla gestione degli oggetti archiviati in [Quarantena virus](#):

- **Limite dimensione per Quarantena virus** - utilizzare il dispositivo di scorrimento per impostare la dimensione massima di [Quarantena virus](#). La dimensione è specificata in maniera proporzionale rispetto alla dimensione del disco locale.
- **Eliminazione automatica file** - questa sezione consente di definire la durata massima di memorizzazione degli oggetti in [Quarantena virus](#) (**Elimina file di più di...giorni**) e il numero massimo di file da memorizzare in [Quarantena virus](#) (**Numero massimo di file da memorizzare**).





### 3.5.13. Autoprotezione di AVG

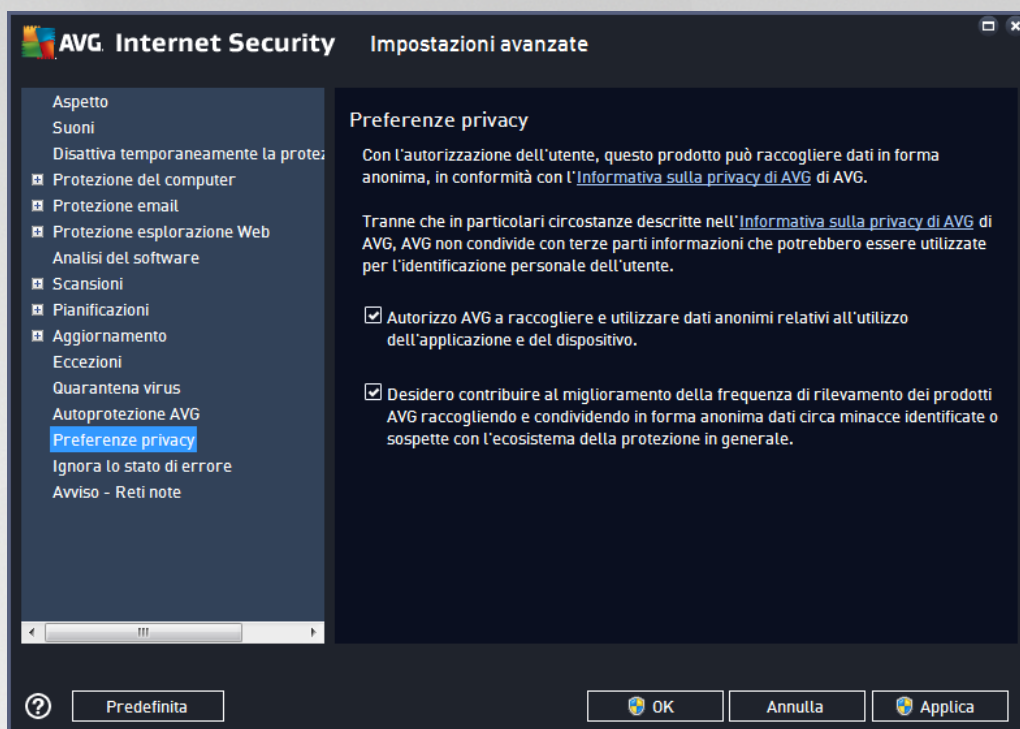


**Autoprotezione di AVG** consente ad **AVG Internet Security** di proteggere i relativi processi, file, chiavi di registro e driver da modifiche o disattivazioni. Il motivo principale per cui si utilizza questo tipo di protezione è che alcune minacce sofisticate tentano di disattivare la protezione antivirus per causare liberamente danni al computer.

**Si consiglia di mantenere questa funzionalità attivata!**

### 3.5.14. Preferenze privacy

La finestra di dialogo **Preferenze privacy** invita l'utente a partecipare al programma per il miglioramento del prodotto AVG per aiutarci ad aumentare il livello di protezione generale in Internet. La segnalazione ci consente di raccogliere informazioni aggiornate sulle minacce più recenti da tutti gli utenti a livello mondiale e di migliorare la protezione per tutti. La segnalazione viene elaborata automaticamente, pertanto non provoca alcun disturbo all'utente. Nei rapporti non vengono inclusi dati personali. La segnalazione delle minacce rilevate è opzionale. Tuttavia si consiglia di mantenere attivata questa opzione. La segnalazione ci aiuta a migliorare la protezione per tutti gli utenti AVG.



Nella finestra di dialogo sono disponibili le seguenti opzioni di impostazione:

- **Desidero contribuire al miglioramento dei prodotti AVG partecipando al Programma di miglioramento del prodotto AVG** (attivata per impostazione predefinita) - per aiutarci a migliorare ulteriormente **AVG Internet Security**, mantenere selezionata questa casella di controllo. Ciò consentirà di segnalare ad AVG tutte le minacce riscontrate. In questo modo saremo in grado di raccogliere informazioni aggiornate sui malware da tutti gli utenti a livello mondiale per offrire un livello di protezione ancora superiore. La segnalazione viene elaborata automaticamente, pertanto non provoca alcun disturbo all'utente e nei rapporti non vengono inclusi dati personali.
  - **Consenti invio dopo conferma dell'utente di dati circa email identificate erroneamente** (attivata per impostazione predefinita) - invia informazioni sui messaggi email identificati erroneamente come spam o sui messaggi di spam non rilevati dal servizio Anti-Spam. Per l'invio di questo tipo di informazioni verrà richiesta la conferma dell'utente.
  - **Consenti invio anonimo di dati circa minacce identificate o sospette** (attivata per impostazione predefinita) - invia informazioni su comportamenti o codici sicuramente pericolosi o sospetti (può trattarsi di un virus, uno spyware o una pagina Web dannosa a cui si sta tentando di accedere) rilevati nel computer.
  - **Consenti invio anonimo di dati circa l'uso del prodotto** (attivata per impostazione predefinita) - invia statistiche di base sull'uso dell'applicazione, ad esempio numero di rilevamenti, scansioni avviate, aggiornamenti riusciti/non riusciti e così via.
- **Permetti verifica cloud dei rilevamenti** (attivata per impostazione predefinita) - le minacce rilevate verranno controllate per verificare l'effettiva presenza di infezioni, in modo da evitare i falsi positivi.
- **Desidero attivare Personalizzazione di AVG per usufruire di un'esperienza utente personalizzata in AVG** (disattivata per impostazione predefinita) - questa funzionalità analizza in

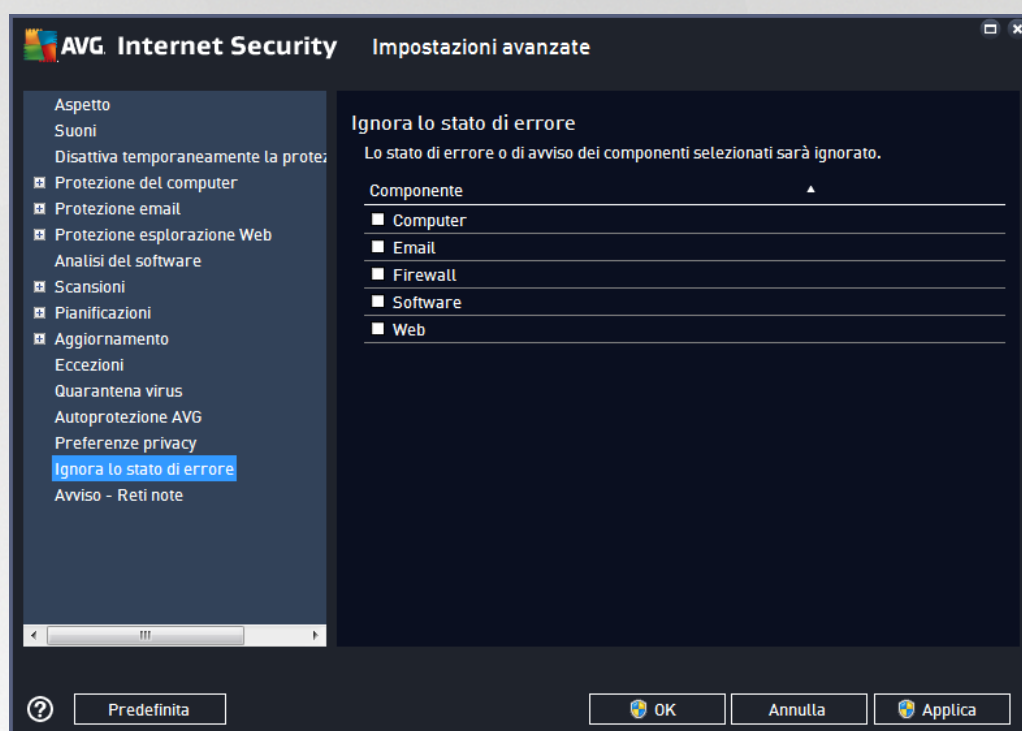




modo anonimo il comportamento dei programmi e delle applicazioni installati nel PC. Grazie a questa analisi, AVG può offrire servizi personalizzati in base alle specifiche esigenze, per assicurare la massima protezione.

### 3.5.15. Ignora lo stato di errore

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



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

- icona dell'area di notifica - quando tutte le parti di AVG funzionano correttamente, l'icona viene visualizzata in quattro colori. Se si verifica un errore, l'icona viene visualizzata con un punto esclamativo giallo,
- una descrizione del problema esistente visualizzata nella sezione [Informazioni sullo stato di protezione](#) della finestra principale di AVG

Potrebbe verificarsi una situazione in cui, per qualsiasi motivo, risulti necessario disattivare un componente temporaneamente. **Questa operazione tuttavia non è consigliabile, si dovrebbe tentare di mantenere attivati tutti i componenti in modo permanente e con la configurazione predefinita.** Se questo si verifica, l'icona dell'area di notifica segnala automaticamente lo stato di errore del componente. In casi del genere, tuttavia, non è possibile parlare di errore effettivo, poiché la condizione è stata indotta deliberatamente dall'utente e si è consapevoli del potenziale rischio. Nel contempo, una volta che viene visualizzata in grigio, l'icona non può più segnalare eventuali errori ulteriori che potrebbero verificarsi.

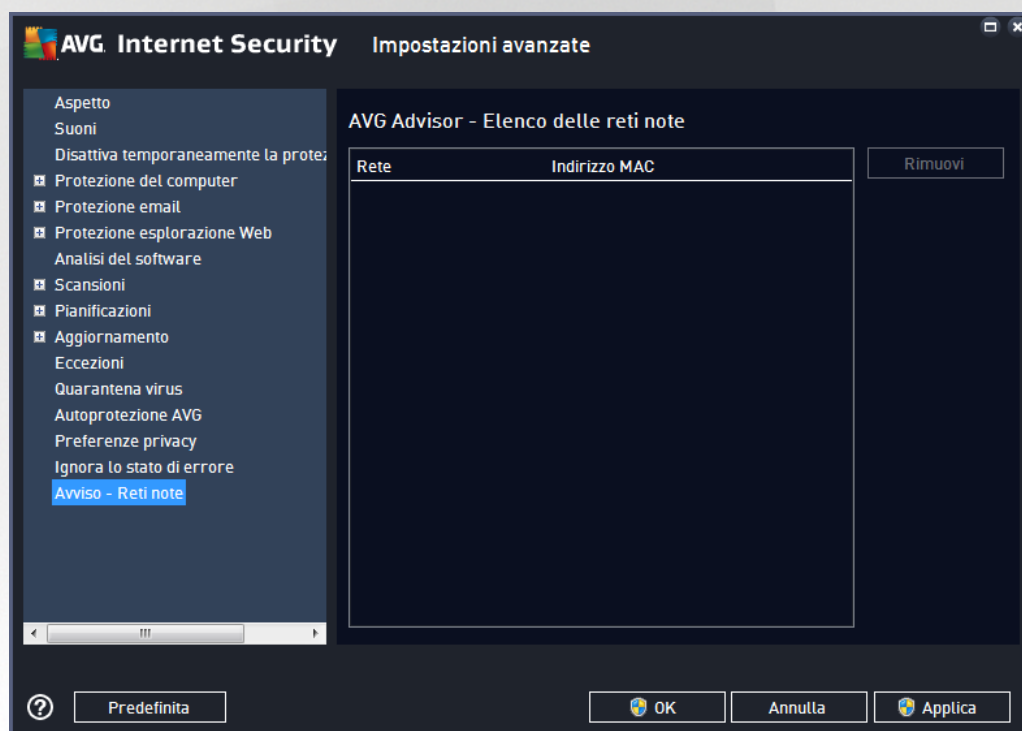
Per gestire situazioni simili, all'interno della finestra di dialogo **Ignora lo stato di errore** è possibile selezionare i componenti che potrebbero trovarsi in stato di errore (o *disattivati*) in merito ai quali non si desidera ricevere informazioni. Selezionare il pulsante **OK** per confermare.



### 3.5.16. Avviso - Reti note

In [AVG Advisor](#) è inclusa una funzionalità che monitora le reti a cui si esegue la connessione e, se viene rilevata una nuova rete (con un nome di rete già utilizzato, che potrebbe generare confusione), visualizza una notifica e suggerisce di verificare la sicurezza della rete. Se si considera sicura la nuova rete, è possibile salvarla in questo elenco (tramite il collegamento visualizzato nella notifica a comparsa di [AVG Advisor](#) nell'area di notifica quando viene rilevata una rete sconosciuta. Per ulteriori dettagli vedere il capitolo su [AVG Advisor](#)). [AVG Advisor](#) memorizzerà gli attributi univoci della rete (in particolare l'indirizzo MAC) e in seguito non visualizzerà la notifica. Ogni rete a cui si esegue la connessione verrà automaticamente considerata come rete conosciuta e aggiunta all'elenco. È possibile eliminare singole voci facendo clic sul pulsante **Rimuovi**: la rete corrispondente verrà nuovamente considerata sconosciuta e potenzialmente non sicura.

In questa finestra di dialogo è possibile controllare quali reti sono considerate conosciute:



**Nota:** la funzione reti conosciute in [AVG Advisor](#) non è supportata in Windows XP a 64 bit.

## 3.6. Impostazioni di Firewall

La finestra di dialogo di configurazione del [Firewall](#) viene aperta in una nuova finestra in cui è possibile impostare parametri avanzati del componente in varie finestre di dialogo. La finestra di dialogo di configurazione viene aperta in una nuova finestra in cui è possibile modificare parametri avanzati del componente in varie finestre di dialogo. È possibile visualizzare la configurazione in modalità di base o avanzata. Quando l'utente visualizza la finestra di dialogo di configurazione per la prima volta, questa viene aperta nella versione di base e consente la modifica dei seguenti parametri:

- [Generale](#)
- [Applicazioni](#)
- [Condivisione file e stampanti](#)





Nella parte inferiore della finestra di dialogo è presente il pulsante **Modalità avanzata**. Far clic sul pulsante per visualizzare ulteriori elementi nell'esplorazione della finestra di dialogo per la configurazione molto avanzata del componente Firewall:

- [Impostazioni avanzate](#)
- [Reti definite](#)
- [Servizi di sistema](#)
- [Log](#)

### 3.6.1. Generale

La finestra di dialogo **Informazioni generali** fornisce una panoramica di tutte le modalità Firewall disponibili. La selezione corrente della modalità Firewall può essere modificata semplicemente selezionando un'altra modalità dal menu.

***Tuttavia, il produttore del software ha impostato tutti i componenti di AVG Internet Security per fornire prestazioni ottimali. A meno che non sussista un motivo valido, si consiglia di non modificare la configurazione predefinita. Le eventuali modifiche alle impostazioni devono essere eseguite solo da utenti esperti.***



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

- **Automatica** - in questa modalità il componente Firewall gestisce tutto il traffico di rete automaticamente. Non verrà richiesto l'intervento dell'utente. Il componente Firewall consentirà la connessione a tutte le applicazioni note e contemporaneamente verrà creata una regola che indica



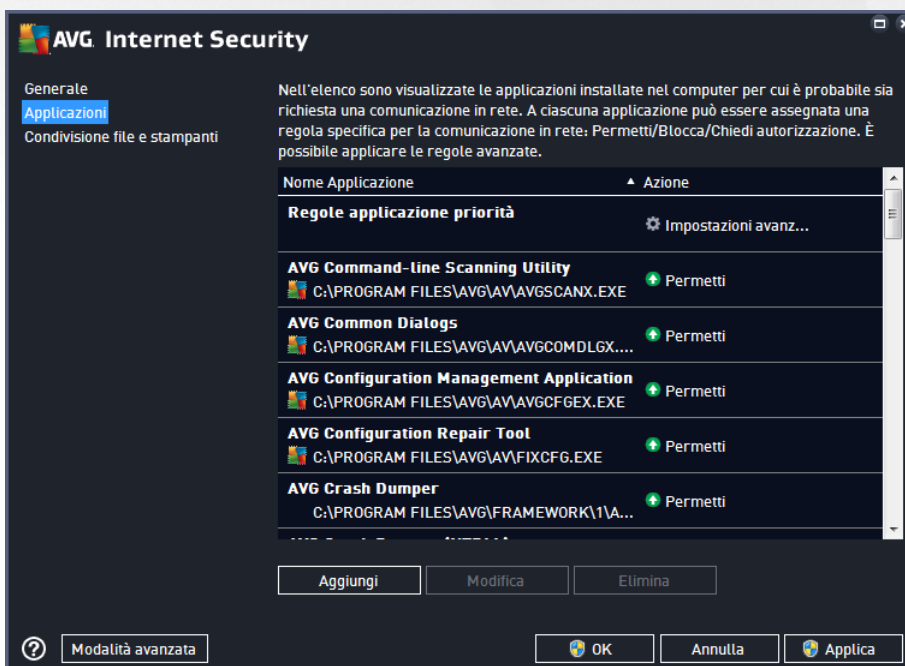
che tale applicazione può connettersi sempre in futuro. Per altre applicazioni, Firewall deciderà se consentire o bloccare la connessione in base al comportamento dell'applicazione. Tuttavia, in questa situazione non verrà creata alcuna regola e l'applicazione verrà controllata nuovamente quando tenta di connettersi. **La modalità automatica è abbastanza discreta ed è consigliata per la maggior parte degli utenti.**

- **Interattiva** - questa modalità è utile se si desidera controllare completamente tutto il traffico di rete in ingresso e in uscita dal computer. Il componente Firewall monitorerà il traffico e notificherà all'utente ogni tentativo di comunicazione o trasferimento dati, permettendo all'utente di consentire o bloccare i tentativi come desidera. Opzione consigliata solo per utenti esperti.
- **Blocca l'accesso a Internet** - la connessione a Internet viene bloccata completamente, è impossibile accedere a Internet e nessuno può accedere al computer dall'esterno. Solo per uso eccezionale e per breve tempo.
- **Disattiva la protezione Firewall** - la disattivazione del Firewall consentirà tutto il traffico di rete in entrata e in uscita dal computer. Di conseguenza, il computer sarà esposto agli attacchi di hacker. Valutare sempre questa opzione con attenzione.

Tenere presente che una modalità automatica specifica è disponibile anche nel Firewall. Questa modalità viene attivata in modo invisibile se i componenti [Protezione del computer](#) o [Analisi del software](#) vengono disattivati rendendo il computer più vulnerabile. In tali casi, il componente Firewall consentirà automaticamente solo le applicazioni note e assolutamente sicure. Per tutti gli altri casi, verrà richiesto all'utente come procedere. Ciò consente di oviare alla disattivazione dei componenti di protezione e di mantenere il computer protetto.

### 3.6.2. Applicazioni




Nella finestra di dialogo **Applicazioni** sono elencate tutte le applicazioni che hanno tentato di comunicare in rete fino ad ora e le icone per l'azione assegnata:



Le applicazioni visualizzate in **Elenco di applicazioni** sono state rilevate sul computer (e dispongono delle rispettive azioni assegnate). È possibile utilizzare i seguenti tipi di azione:





-  - consenti comunicazione per tutte le reti
-  - blocca comunicazione
-  - impostazioni avanzate definite

**Tenere presente che è possibile rilevare solo le applicazioni già installate. Per impostazione predefinita, quando la nuova applicazione tenta di connettersi in rete per la prima volta, il componente Firewall crea automaticamente una regola in base al [Database attendibile](#) oppure chiede all'utente se consentire o bloccare la comunicazione. Nel secondo caso, sarà possibile salvare la risposta come regola permanente (che verrà quindi elencata in questa finestra di dialogo).**

Naturalmente, è anche possibile definire immediatamente le regole per la nuova applicazione. In questa finestra di dialogo fare clic su **Aggiungi** e immettere i dettagli dell'applicazione.

Oltre alle applicazioni, nell'elenco sono incluse anche due voci speciali. **Regole per applicazione prioritaria** (nella parte superiore dell'elenco). Queste regole sono preferenziali e vengono sempre applicate prima delle regole di ogni singola applicazione. **Regole per altre applicazioni** (nella parte inferiore dell'elenco). Queste regole sono utilizzate come "ultima istanza" quando non si applicano regole di applicazioni specifiche, ad esempio per un'applicazione sconosciuta e non definita. Selezionare l'azione che deve essere attivata se un'applicazione effettuasse un tentativo di comunicazione sulla rete: Blocca (la comunicazione sarà sempre bloccata), Consenti (la comunicazione sarà consentita su tutte le reti), Richiedi (l'utente dovrà specificare se la comunicazione deve essere consentita o bloccata). **Questi elementi presentano opzioni di impostazione diverse dalle applicazioni comuni e sono destinati esclusivamente agli utenti esperti. Si consiglia di non modificare le impostazioni.**

### **Pulsanti di controllo**

Per modificare l'elenco, utilizzare i seguenti pulsanti di controllo:

- **Aggiungi** - consente di aprire una finestra di dialogo vuota per la definizione di nuove regole delle applicazioni.
- **Modifica** - consente di aprire la stessa finestra di dialogo completa di dati per la modifica di un insieme di regole per un'applicazione esistente.
- **Elimina** - consente di rimuovere dall'elenco l'applicazione selezionata.

### **3.6.3. Condivisione file e stampanti**

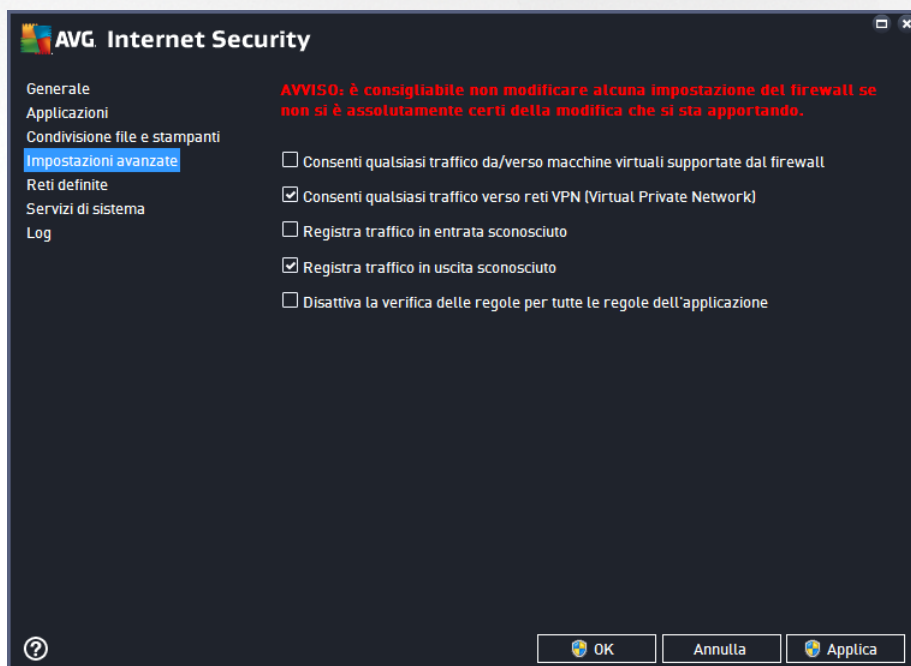
Condivisione di file e stampanti significa condividere qualsiasi file o cartella contrassegnato come "Condiviso" in Windows, in unità disco comuni, stampanti, scanner e dispositivi simili. È preferibile condividere tali elementi solo all'interno di reti considerate sicure (ad esempio a casa, in ufficio o a scuola). Tuttavia, se si è connessi a una rete pubblica (ad esempio, al Wi-Fi dell'aeroporto o di un Internet Point), è consigliabile non condividere nulla. AVG Firewall può bloccare o consentire facilmente la condivisione e permettere all'utente di salvare la scelta eseguita per le reti già visitate.



Nella finestra di dialogo **Condivisione file e stampanti** è possibile modificare la configurazione della condivisione file e stampanti e le reti attualmente connesse. Con Windows XP, il nome della rete corrisponde alla denominazione scelta per la rete specifica durante la prima connessione. Con Windows Vista e versioni successive, il nome della rete viene ricavato automaticamente dal Centro connessioni di rete e condivisione.

### 3.6.4. Impostazioni avanzate

**Le modifiche nella finestra di dialogo *Impostazioni avanzate* sono riservate *ESCLUSIVAMENTE* agli *UTENTI ESPERTI*.**







La finestra di dialogo **Impostazioni avanzate** consente di attivare/disattivare i seguenti parametri del componente Firewall:

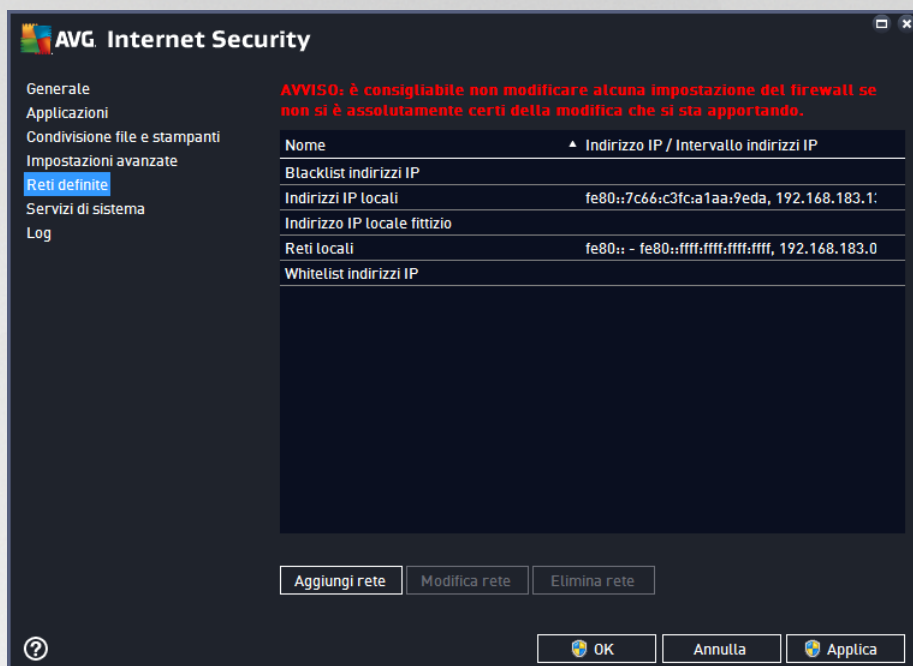
- **Consenti qualsiasi traffico da/verso macchine virtuali supportate dal firewall** - supporto per la connessione di rete in macchine virtuali come VMware.
- **Consenti qualsiasi traffico verso reti VPN (Virtual Private Network)** - supporto per connessioni VPN (*utilizzato per connettersi a computer remoti*).
- **Registra traffico sconosciuto in entrata/in uscita** - tutti i tentativi di comunicazione (*entranti/uscenti*) da parte di applicazioni sconosciute verranno registrati nel [Log Firewall](#).
- **Disattiva la verifica delle regole per tutte le regole dell'applicazione** - Firewall monitora costantemente tutti file coperti dalle regole dell'applicazione. Quando si apporta una modifica al file binario, Firewall tenta di confermare nuovamente la credibilità dell'applicazione utilizzando metodi standard, ovvero mediante il controllo del certificato, la ricerca dell'applicazione nel [database delle applicazioni attendibili](#) e così via. Se non è possibile considerare l'applicazione sicura, Firewall si comporterà in base alla [modalità selezionata](#):
  - se Firewall è configurato in [Modalità automatica](#), l'applicazione viene consentita per impostazione predefinita;
  - se Firewall è configurato in [Modalità interattiva](#), l'applicazione viene bloccata e viene visualizzata una finestra di dialogo che chiede all'utente di decidere come gestire l'applicazione.

È anche possibile definire separatamente la procedura di gestione desiderata per specifiche applicazioni nella finestra di dialogo [Applicazioni](#).



### 3.6.5. Reti definite

Le eventuali modifiche alla finestra di dialogo *Reti definite* sono riservate **ESCLUSIVAMENTE** agli **UTENTI ESPERTI**.



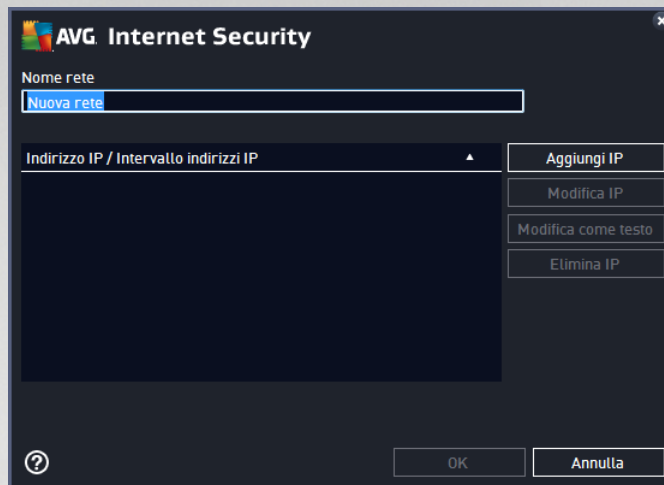
Nella finestra di dialogo *Reti definite* è disponibile un elenco di tutte le reti a cui è connesso il computer. L'elenco fornisce le seguenti informazioni su ciascuna rete rilevata:

- **Reti** - fornisce l'elenco dei nomi di tutte le reti a cui è connesso il computer.
- **Intervallo indirizzi IP** - ogni rete verrà rilevata automaticamente e specificata sotto forma di intervallo di indirizzi IP.

#### Pulsanti di controllo

- **Aggiungi rete** - consente di aprire una nuova finestra di dialogo in cui è possibile modificare i parametri della rete appena definita, ovvero specificare il **nome della rete** e l'**intervallo di indirizzi IP**.





- **Modifica rete** - consente di aprire la finestra di dialogo **Proprietà rete** (vedere sopra) dove è possibile modificare i parametri di una rete già definita (questa finestra di dialogo è identica alla finestra di dialogo per l'aggiunta di nuove reti, vedere la descrizione nel paragrafo precedente).
- **Elimina rete** - consente di rimuovere il riferimento a una rete selezionata dall'elenco delle reti.

### 3.6.6. Servizi di sistema

**Le modifiche alla finestra di dialogo Protocolli e servizi di sistema sono riservate ESCLUSIVAMENTE agli UTENTI ESPERTI.**



La finestra di dialogo **Protocolli e servizi di sistema** elenca i protocolli e i servizi di sistema standard di Windows che potrebbero dover comunicare sulla rete. Il grafico presenta le seguenti colonne:

- **Protocolli e servizi di sistema** - questa colonna mostra il nome del rispettivo servizio di sistema.

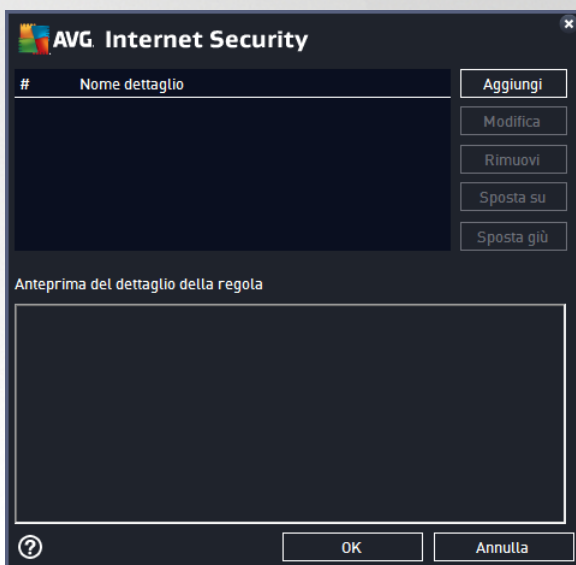


- **Azione** - questa colonna mostra un'icona per l'azione assegnata:
  - Consenti comunicazione per tutte le reti
  - Blocca comunicazione

Per modificare le impostazioni delle voci dell'elenco (*incluse le azioni assegnate*), fare clic con il pulsante destro del mouse sulla voce desiderata e selezionare **Modifica**. **Tuttavia, la modifica delle regole di sistema dovrebbe essere eseguita solo da utenti avanzati. È consigliabile non modificare le regole di sistema.**

### Regole di sistema definite dall'utente

Per aprire una nuova finestra di dialogo per la definizione di una regola dei servizi di sistema personalizzata (*vedere la seguente immagine*), selezionare il pulsante **Gestisci regole di sistema dell'utente**. La stessa finestra di dialogo verrà visualizzata se si decide di modificare la configurazione di qualsiasi elemento presente nell'elenco dei protocolli e dei servizi di sistema. La sezione superiore di questa finestra di dialogo mostra una panoramica di tutti i dettagli della regola di sistema modificata, la sezione inferiore mostra quindi il dettaglio selezionato. I dettagli delle regole possono essere modificati, aggiunti o eliminati tramite gli appositi pulsanti:



**Tenere presente che queste impostazioni delle regole dettagliate sono avanzate e destinate innanzitutto agli amministratori di rete che necessitano del controllo completo della configurazione del componente Firewall. Se non si conoscono i tipi di protocollo di comunicazione, i numeri delle porte di rete, le definizioni degli indirizzi IP e così via, non modificare queste impostazioni. Se fosse necessario modificare la configurazione, consultare i file della Guida della rispettiva finestra di dialogo per dettagli specifici.**

### 3.6.7. Log

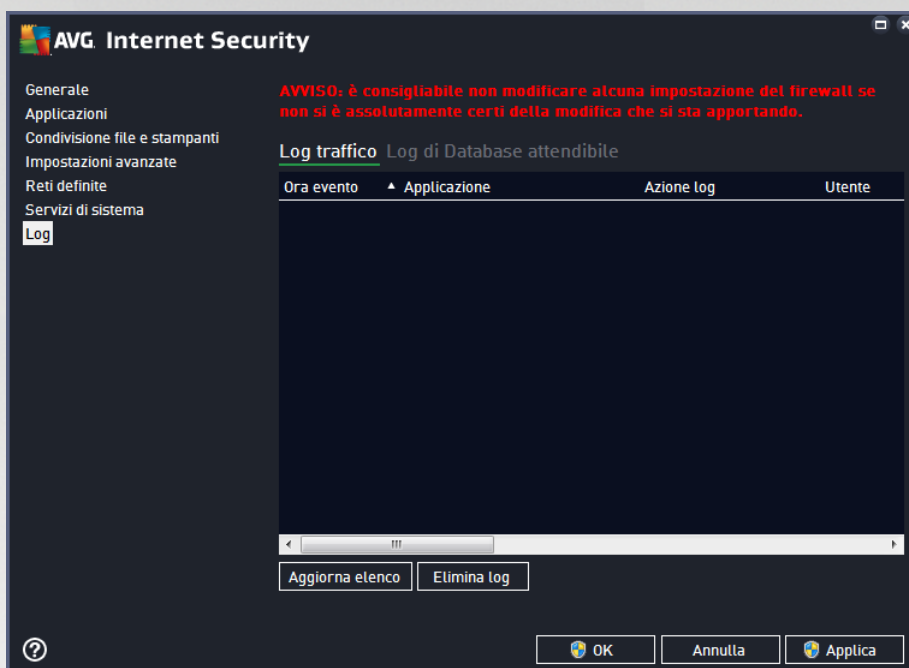
**Le eventuali modifiche alla finestra di dialogo Log sono riservate ESCLUSIVAMENTE agli UTENTI ESPERTI.**

La finestra di dialogo **Log** consente di visualizzare l'elenco di tutte le azioni e gli eventi registrati di Firewall con una descrizione dettagliata dei parametri rilevanti mostrata in due schede:

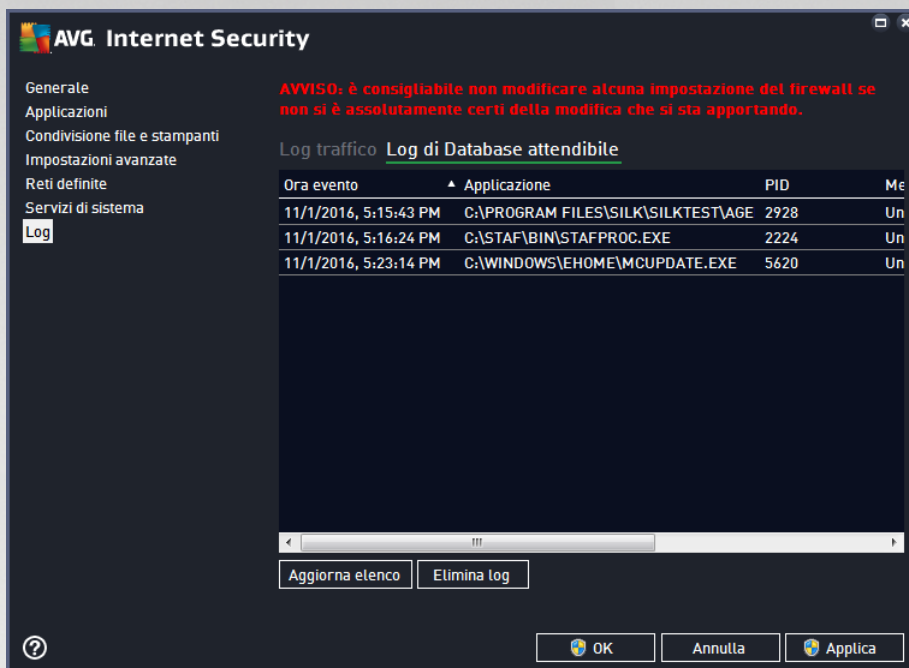




- **Log traffico** - questa scheda fornisce informazioni sull'attività di tutte le applicazioni che hanno tentato di connettersi alla rete. Per ognuna di queste, saranno incluse informazioni relative a ora dell'evento, nome dell'applicazione, rispettiva azione log, nome utente, PID, direzione del traffico, tipo di protocollo, numeri delle porte remote e locali e informazioni sull'indirizzo IP remoto e locale.



- **Log database attendibile** - il *Database attendibile* è un database interno di AVG che raccoglie informazioni sulle applicazioni certificate e attendibili che saranno sempre autorizzate a comunicare online. La prima volta in cui una nuova applicazione tenta di connettersi alla rete (*ossia quando non è ancora stata specificata alcuna regola firewall per tale applicazione*), è necessario stabilire se la comunicazione di rete deve essere consentita per tale applicazione. Innanzitutto, AVG effettua una ricerca nel *Database attendibile*. Se l'applicazione è elencata, sarà automaticamente autorizzata ad accedere alla rete. Se nel database non sono presenti informazioni sull'applicazione, verrà richiesto in una nuova finestra di dialogo se si desidera autorizzare l'applicazione ad accedere alla rete.



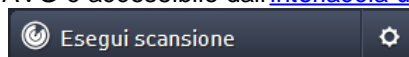
### Pulsanti di controllo

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

## 3.7. Scansione AVG

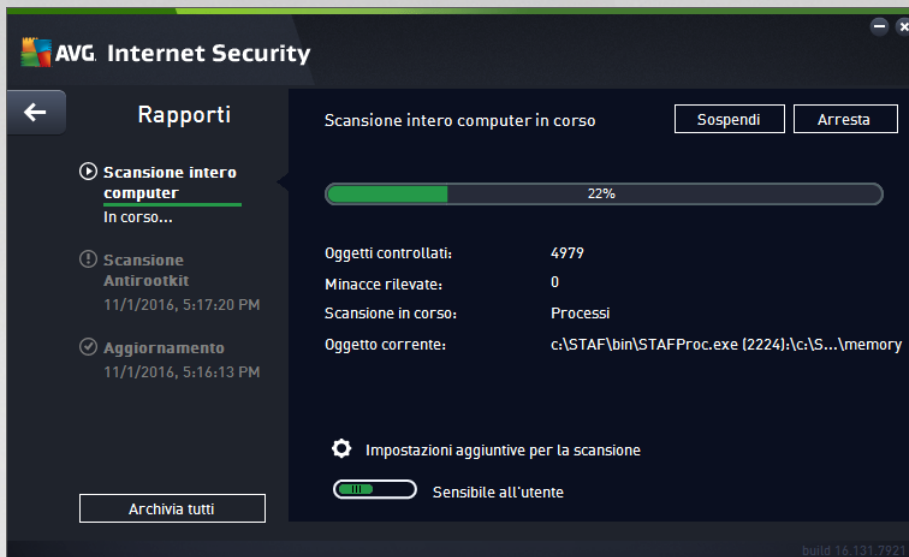
Per impostazione predefinita, **AVG Internet Security** non esegue alcuna scansione, poiché dopo la scansione iniziale (*che all'utente viene richiesto di avviare*), il computer dovrebbe essere perfettamente protetto dai componenti permanenti di **AVG Internet Security** che sono sempre attivi e non lasciano entrare codice dannoso nel sistema. Naturalmente, è possibile [pianificare l'esecuzione di una scansione](#) a intervalli regolari o avviare manualmente una scansione in qualsiasi momento in base alle esigenze.

L'interfaccia di scansione di AVG è accessibile dall'[interfaccia utente principale](#) tramite il pulsante suddiviso graficamente in due sezioni:



- **Esegui scansione** - fare clic su questo pulsante per avviare la [Scansione intero computer](#) e visualizzare l'avanzamento e i relativi risultati nella finestra [Rapporti](#), che viene aperta automaticamente:





- **Opzioni** - fare clic su questo pulsante (*visualizzato graficamente come tre linee orizzontali su sfondo verde*) per aprire la finestra di dialogo **Opzioni di scansione**, dove è possibile [gestire le scansioni pianificate](#) e modificare i parametri di [Scansione intero computer](#) / [Scansione file o cartelle](#).



Nella finestra di dialogo **Opzioni di scansione** sono disponibili tre sezioni principali per la configurazione delle scansioni:

- **Gestione scansioni pianificate** - fare clic su questa opzione per aprire una nuova [finestra di dialogo con una panoramica di tutte le scansioni pianificate](#). Se non sono state definite scansioni personalizzate, nell'elenco sarà visualizzata solo una scansione pianificata predefinita dal fornitore del software. Per impostazione predefinita, tale scansione è disattivata. Per attivarla, fare clic con il pulsante destro del mouse sull'opzione *Abilita attività* dal menu di scelta rapida. Dopo aver abilitato la scansione pianificata, è possibile [modificarne la configurazione](#) utilizzando il pulsante *Modifica pianificazione scansione*. Inoltre, è possibile fare clic sul pulsante *Aggiungi scansione pianificata* per creare e pianificare una scansione personalizzata.



- **Scansione intero computer / Impostazioni** - questo pulsante è suddiviso in due sezioni. Fare clic sull'opzione *Scansione intero computer* per avviare immediatamente la scansione dell'intero computer (per ulteriori dettagli, vedere il capitolo [Scansioni predefinite / Scansione intero computer](#)). Facendo clic sulla sezione *Impostazioni* è possibile accedere alla [finestra di dialogo di configurazione della scansione intero computer](#).
- **Scansione file o cartelle / Impostazioni** - anche questo pulsante è suddiviso in due sezioni. Fare clic sull'opzione *Scansione file o cartelle* per avviare immediatamente la scansione delle aree selezionate del computer (per ulteriori dettagli, vedere il capitolo [Scansioni predefinite / Scansione file o cartelle](#)). Facendo clic sulla sezione *Impostazioni* è possibile accedere alla [finestra di dialogo di configurazione della scansione file o cartelle](#).
- **Esegui la ricerca di rootkit nel computer / Impostazioni** - fare clic sulla sezione di sinistra del pulsante denominata *Esegui la ricerca di rootkit nel computer* per avviare immediatamente la ricerca di rootkit (per ulteriori dettagli, vedere il capitolo [Scansioni predefinite / Esegui la ricerca di rootkit nel computer](#)). Facendo clic sulla sezione *Impostazioni* è possibile accedere alla [finestra di dialogo di configurazione della ricerca di rootkit](#).

### 3.7.1. Scansioni predefinite

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

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

#### 3.7.1.1. Scansione intero computer

**Scansione intero computer** consente di eseguire scansioni dell'intero computer per il rilevamento di possibili infezioni e/o di applicazioni potenzialmente indesiderate. Questo controllo eseguirà la scansione di tutti i dischi rigidi nel computer, rileverà e correggerà i virus trovati oppure sposterà l'infezione rilevata in [Quarantena virus](#). È necessario pianificare la scansione dell'intero computer almeno una volta la settimana.

#### Avvio della scansione

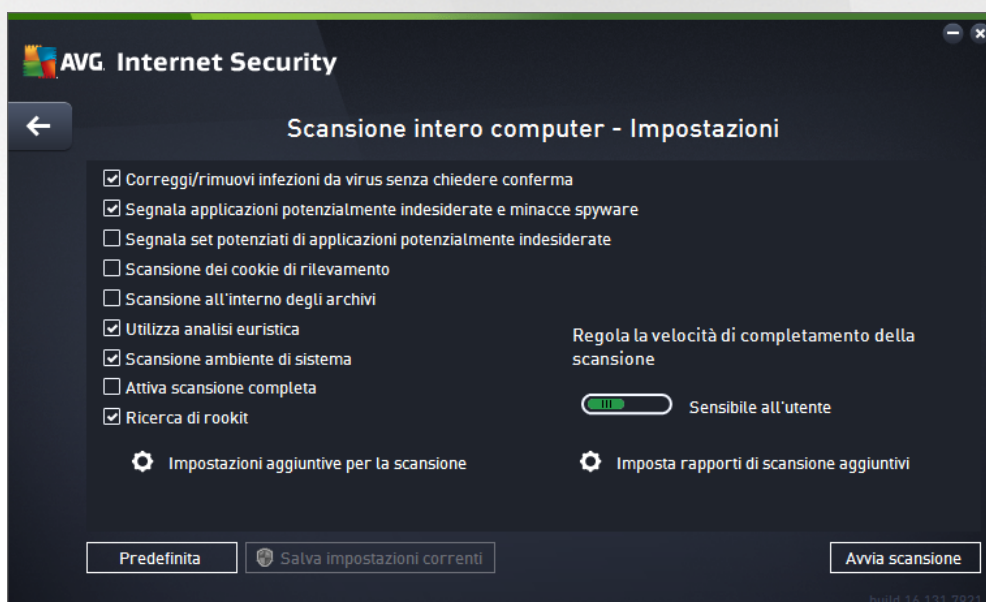
La **Scansione intero computer** può essere avviata direttamente dall'[interfaccia utente principale](#) facendo clic sul pulsante **Esegui scansione**. Non è necessario configurare ulteriori impostazioni specifiche per questo tipo di scansione. La scansione verrà avviata immediatamente. Nella finestra di dialogo **Scansione intero computer** (vedere la schermata) è possibile visualizzare l'avanzamento della scansione e i relativi risultati. La scansione può essere temporaneamente interrotta (**Sospendi**) oppure annullata (**Arresta**) se necessario.





### Modifica della configurazione della scansione

È possibile modificare la configurazione di **Scansione intero computer** nella finestra di dialogo **Scansione intero computer - Impostazioni** (tale finestra è accessibile tramite il collegamento **Impostazioni per Scansione intero computer** nella finestra **Opzioni di scansione**). **Si consiglia di mantenere le impostazioni predefinite e di modificarle solo se esiste un reale motivo per farlo.**



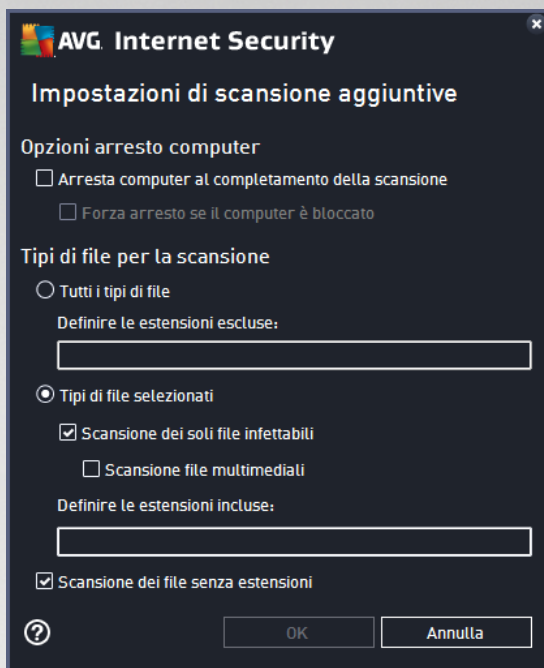
Nell'elenco dei parametri di scansione è possibile attivare/disattivare parametri specifici in base alle esigenze:

- **Correggi/Rimuovi infezioni da virus senza richiedere conferma** (attivata per impostazione predefinita) - se viene identificato un virus durante la scansione, può essere corretto automaticamente se è disponibile una soluzione. Se il file infetto non può essere corretto automaticamente, l'oggetto infetto verrà spostato in [Quarantena virus](#).



- **Segnala applicazioni potenzialmente indesiderate e minacce spyware** (attivata per impostazione predefinita) - selezionare questa casella di controllo per attivare la scansione per ricercare sia spyware che virus. Gli spyware rappresentano una categoria di malware anomala: anche se solitamente costituiscono un rischio per la sicurezza, alcuni di questi programmi possono essere installati intenzionalmente. Si consiglia di mantenere questa funzionalità attivata in quanto consente di aumentare la protezione del computer.
- **Segnala set potenziati di applicazioni potenzialmente indesiderate** (disattivata per impostazione predefinita) - selezionare questa casella di controllo per rilevare pacchetti estesi di spyware, ovvero programmi perfettamente normali e innocui al momento dell'acquisto diretto presso il produttore, ma utilizzabili a scopi dannosi successivamente. Si tratta di una precauzione aggiuntiva che aumenta ulteriormente la protezione del computer, ma che potrebbe bloccare programmi legittimi, pertanto l'opzione è disattivata per impostazione predefinita.
- **Scansione dei cookie di rilevamento** (disattivata per impostazione predefinita) - questo parametro specifica che i cookie devono essere rilevati (*i cookie HTTP vengono utilizzati per autenticare, rilevare e mantenere informazioni specifiche sugli utenti, quali le preferenze dei siti o il contenuto dei carrelli elettronici*).
- **Scansione all'interno degli archivi** (disattivata per impostazione predefinita) - questo parametro specifica che la scansione deve controllare tutti i file inclusi all'interno di un archivio, quali ZIP, RAR e così via.
- **Usa analisi euristiche** (attivata per impostazione predefinita - l'analisi euristica (*emulazione dinamica delle istruzioni dell'oggetto sottoposto a scansione in un ambiente informatico virtuale*) sarà uno dei metodi utilizzati per il rilevamento di virus durante la scansione.
- **Scansione ambiente di sistema** (attivata per impostazione predefinita) - la scansione verrà eseguita anche sulle aree di sistema del computer.
- **Attiva scansione completa** (disattivata per impostazione predefinita) - in situazioni specifiche (*se si sospetta che il computer sia stato infettato*) per maggiore sicurezza è possibile selezionare questa opzione per attivare gli algoritmi di scansione più completi che esamineranno anche le aree del computer che difficilmente vengono infettate. Tenere presente tuttavia che questo metodo è piuttosto dispendioso in termini di tempo.
- **Ricerca di rootkit** (attivata per impostazione predefinita): include la scansione Antirootkit nella scansione dell'intero computer. È anche possibile avviare la [Scansione Antirootkit](#) separatamente.
- **Impostazioni di scansione aggiuntive** - il collegamento consente di aprire una nuova finestra di dialogo Impostazioni di scansione aggiuntive in cui è possibile specificare i parametri descritti di seguito.

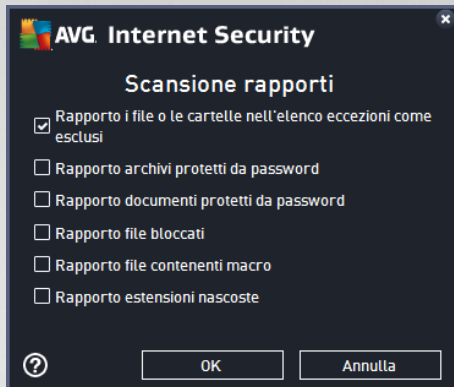




- **Opzioni arresto computer** - consente di decidere se il computer deve essere arrestato automaticamente al termine del processo di scansione. Dopo aver confermato questa opzione (**Arresta computer al completamento della scansione**), viene attivata una nuova opzione che consente l'arresto del computer anche se è correntemente bloccato (**Forza arresto se il computer è bloccato**).
- **Tipi di file per la scansione** - specificare se si desidera sottoporre a scansione:
  - **Tutti i tipi di file** con l'opzione per definire le eccezioni fornendo un elenco di estensioni di file separate da virgola da non sottoporre a scansione.
  - **Tipi di file selezionati** - è possibile specificare che si desidera sottoporre a scansione solo i file potenzialmente infettabili (*i file che non possono essere infettati non verranno sottoposti a scansione, ad esempio alcuni file di testo normale o altri file non eseguibili*), inclusi i file multimediali (*file video e audio; se non si seleziona questa casella, il tempo di scansione risulterà ulteriormente ridotto, poiché questi file sono spesso di grandi dimensioni e non facilmente infettabili dai virus*). Anche in questo caso, è possibile specificare tramite le estensioni quali file devono essere sempre sottoposti a scansione.
  - Facoltativamente, è possibile effettuare la **scansione dei file senza estensioni**: questa opzione è attivata per impostazione predefinita e si consiglia di non modificarla a meno che non siano presenti motivi validi per farlo. I file senza estensione sono piuttosto sospetti e devono essere sempre sottoposti a scansione.
- **Regola la velocità di completamento della scansione** - è possibile utilizzare il dispositivo di scorrimento per modificare la priorità del processo di scansione. Per impostazione predefinita, questa opzione è impostata sul livello *Sensibile all'utente* per l'utilizzo automatico delle risorse. In alternativa, è possibile eseguire il processo di scansione più lentamente in modo da ridurre al minimo il carico sulle risorse di sistema (*utile quando è necessario lavorare al computer indipendentemente dalla durata della scansione*) o più velocemente con un utilizzo delle risorse di sistema più elevato (*utile ad esempio quando ci si allontana temporaneamente dal computer*).



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



**Avviso:** queste impostazioni di scansione sono identiche ai parametri di una nuova scansione, definita come descritto nel capitolo [Scansione AVG / Pianificazione di scansioni / Scansione da eseguire](#). Se si decide di modificare la configurazione predefinita di **Scansione intero computer**, è possibile salvare le nuove impostazioni come configurazione predefinita da utilizzare per tutte le altre scansioni dell'intero computer.

### 3.7.1.2. Scansione file o cartelle

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

#### Avvio della scansione

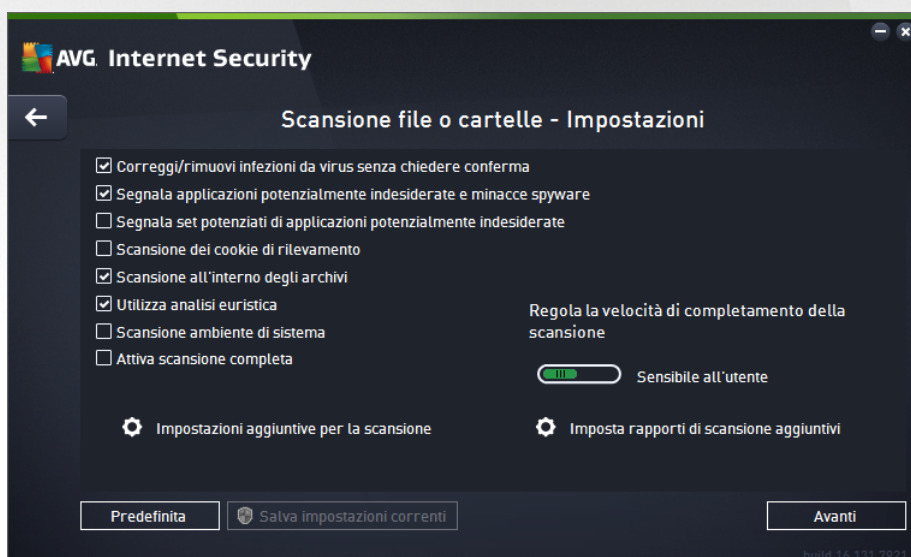
È possibile avviare la **Scansione file o cartelle** direttamente dalla finestra di dialogo [Opzioni di scansione](#) facendo clic sul pulsante **Scansione file o cartelle**. Viene aperta una nuova finestra di dialogo **Selezionare file o cartelle specifiche per la scansione**. Nella struttura del computer selezionare le cartelle da sottoporre a scansione. Il percorso di ciascuna cartella selezionata verrà generato automaticamente e visualizzato nella casella di testo nella parte superiore della finestra di dialogo. È inoltre possibile sottoporre a scansione una specifica cartella escludendo tutte le relative sottocartelle, a questo scopo scrivere un segno meno "-" all'inizio del percorso generato automaticamente (*vedere la schermata*). Per escludere l'intera cartella dalla scansione, utilizzare il parametro "!". Infine, per avviare la scansione, selezionare il pulsante **Avvia scansione**. Il processo di scansione è praticamente identico a quello di [Scansione intero computer](#).





### Modifica della configurazione della scansione

È possibile modificare la configurazione di **Scansione file o cartelle** nella finestra di dialogo **Scansione file o cartelle - Impostazioni** (tale finestra è accessibile tramite il collegamento **Impostazioni per Scansione file o cartelle** nella finestra [Opzioni di scansione](#)). **Si consiglia di mantenere le impostazioni predefinite e di modificarle solo se esiste un reale motivo per farlo.**



Nell'elenco dei parametri di scansione è possibile attivare/disattivare parametri specifici in base alle esigenze:

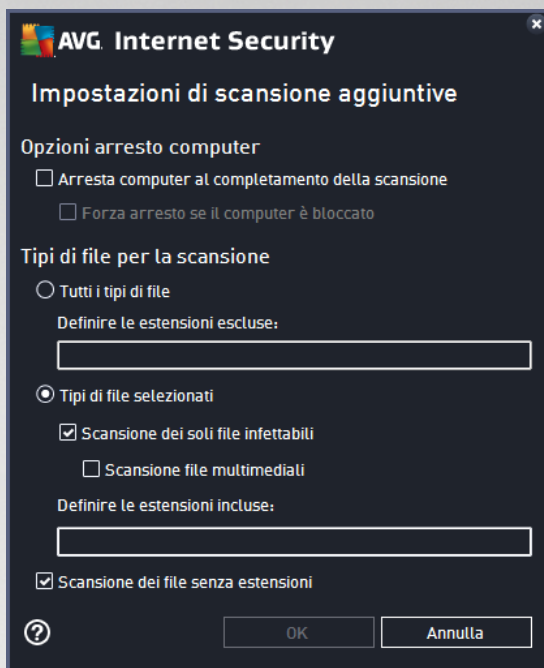
- **Correggi/Rimuovi infezioni da virus senza richiedere conferma** (attivata per impostazione predefinita): Se viene identificato un virus durante la scansione può essere corretto automaticamente se è disponibile una soluzione. Se il file infetto non può essere corretto automaticamente, l'oggetto infetto verrà spostato in [Quarantena virus](#).
- **Segnala applicazioni potenzialmente indesiderate e minacce spyware** (attivata per impostazione



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

- **Segnala set potenziati di applicazioni potenzialmente indesiderate** (*disattivata per impostazione predefinita*): Selezionare per rilevare pacchetti estesi di spyware, ovvero programmi perfettamente normali e innocui al momento dell'acquisto diretto presso il produttore, ma utilizzabili a scopi dannosi successivamente. Si tratta di una precauzione aggiuntiva che aumenta ulteriormente la protezione del computer, ma che potrebbe bloccare programmi legittimi, pertanto l'opzione è disattivata per impostazione predefinita.
- **Scansione dei cookie di rilevamento** (*disattivata per impostazione predefinita*): Questo parametro specifica che i cookie devono essere rilevati (*i cookie HTTP vengono utilizzati per autenticare, rilevare e mantenere informazioni specifiche sugli utenti, quali le preferenze dei siti o il contenuto dei carrelli elettronici*).
- **Scansione all'interno degli archivi** (*attivata per impostazione predefinita*): Questo parametro specifica che la scansione deve controllare tutti i file inclusi all'interno di un archivio, quali ZIP, RAR e così via.
- **Usa analisi euristiche** (*attivata per impostazione predefinita*): l'analisi euristica (*emulazione dinamica delle istruzioni dell'oggetto sottoposto a scansione in un ambiente informatico virtuale*) sarà uno dei metodi utilizzati per il rilevamento di virus durante la scansione.
- **Scansione ambiente di sistema** (*disattivata per impostazione predefinita*): la scansione verrà eseguita anche sulle aree di sistema del computer.
- **Attiva scansione completa** (*disattivata per impostazione predefinita*): in situazioni specifiche (*se si sospetta che il computer sia stato infettato*) per maggiore sicurezza è possibile selezionare questa opzione per attivare gli algoritmi di scansione più completi che esamineranno anche le aree del computer che difficilmente vengono infettate. Tenere presente tuttavia che questo metodo è piuttosto dispendioso in termini di tempo.
- **Impostazioni di scansione aggiuntive** - il collegamento consente di aprire una nuova finestra di dialogo **Impostazioni di scansione aggiuntive** in cui è possibile specificare i parametri descritti di seguito.

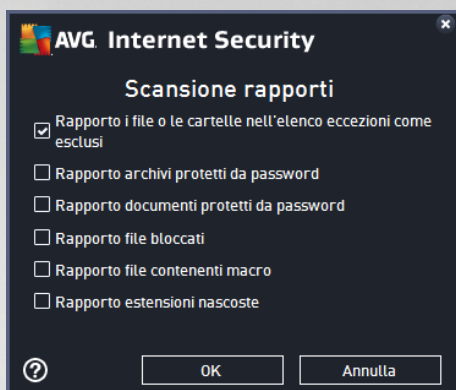




- **Opzioni arresto computer** - consente di decidere se il computer deve essere arrestato automaticamente al termine del processo di scansione. Dopo aver confermato questa opzione (**Arresta computer al completamento della scansione**), viene attivata una nuova opzione che consente l'arresto del computer anche se è correntemente bloccato (**Forza arresto se il computer è bloccato**).
- **Tipi di file per la scansione** - specificare se si desidera sottoporre a scansione:
  - **Tutti i tipi di file** con l'opzione per definire le eccezioni fornendo un elenco di estensioni di file separate da virgola da non sottoporre a scansione.
  - **Tipi di file selezionati** - è possibile specificare che si desidera sottoporre a scansione solo i file potenzialmente infettabili (*i file che non possono essere infettati non verranno sottoposti a scansione, ad esempio alcuni file di testo normale o altri file non eseguibili*), inclusi i file multimediali (*file video e audio; se non si seleziona questa casella, il tempo di scansione risulterà ulteriormente ridotto, poiché questi file sono spesso di grandi dimensioni e non facilmente infettabili dai virus*). Anche in questo caso, è possibile specificare tramite le estensioni quali file devono essere sempre sottoposti a scansione.
  - Facoltativamente, è possibile effettuare la **scansione dei file senza estensioni**: questa opzione è attivata per impostazione predefinita e si consiglia di non modificarla a meno che non siano presenti motivi validi per farlo. I file senza estensione sono piuttosto sospetti e devono essere sempre sottoposti a scansione.
- **Regola la velocità di completamento della scansione** - è possibile utilizzare il dispositivo di scorrimento per modificare la priorità del processo di scansione. Per impostazione predefinita, questa opzione è impostata sul livello *Sensibile all'utente* per l'utilizzo automatico delle risorse. In alternativa, è possibile eseguire il processo di scansione più lentamente in modo da ridurre al minimo il carico sulle risorse di sistema (*utile quando è necessario lavorare al computer indipendentemente dalla durata della scansione*) o più velocemente con un utilizzo delle risorse di sistema più elevato (*utile ad esempio quando ci si allontana temporaneamente dal computer*).



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



**Avviso:** queste impostazioni di scansione sono identiche ai parametri di una nuova scansione, definita come descritto nel capitolo [Scansione AVG / Pianificazione di scansioni / Scansione da eseguire](#). Se si decide di modificare la configurazione predefinita di **Scansione file o cartelle** è possibile salvare le nuove impostazioni come configurazione predefinita da utilizzare per tutte le altre scansioni di file o cartelle specifiche. Inoltre, questa configurazione verrà utilizzata come modello per tutte le nuove scansioni pianificate ([tutte le scansioni personalizzate si basano sulla configurazione corrente di Scansione file o cartelle](#)).

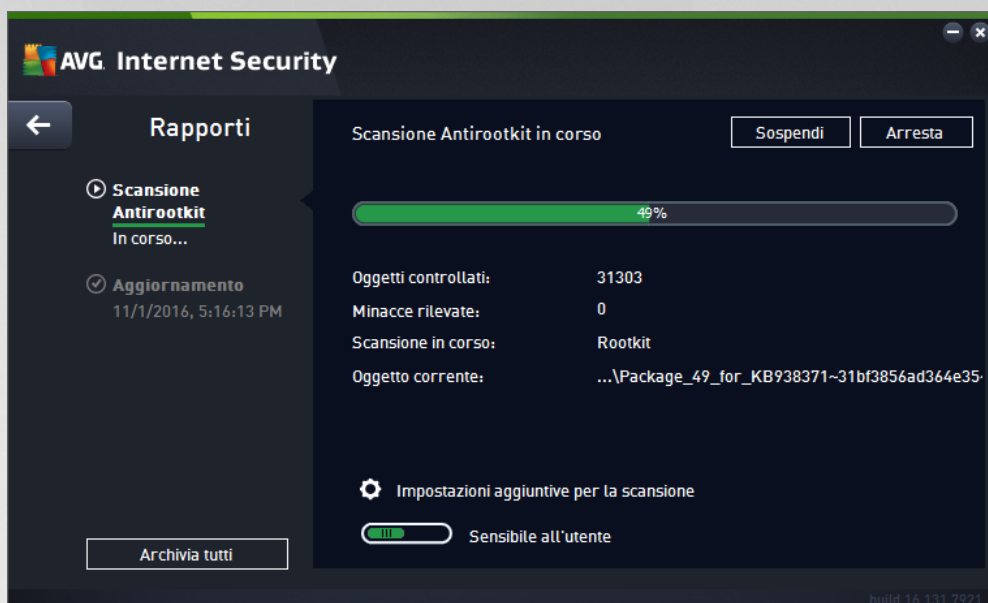
### 3.7.1.3. Ricerca di rootkit nel computer

**Esegui la ricerca di rootkit nel computer** consente di rilevare e rimuovere efficacemente i rootkit dannosi, ovvero programmi e tecnologie che possono camuffare la presenza di software dannoso nel computer. Un rootkit è progettato per assumere il controllo di base di un sistema senza autorizzazione da parte dei proprietari e dei gestori legittimi del sistema. La scansione è in grado di rilevare i rootkit in base a un gruppo predefinito di regole. Se viene individuato un rootkit, non significa necessariamente che sia infetto. Talvolta i rootkit vengono utilizzati come driver o fanno parte di applicazioni regolari.

#### Avvio della scansione

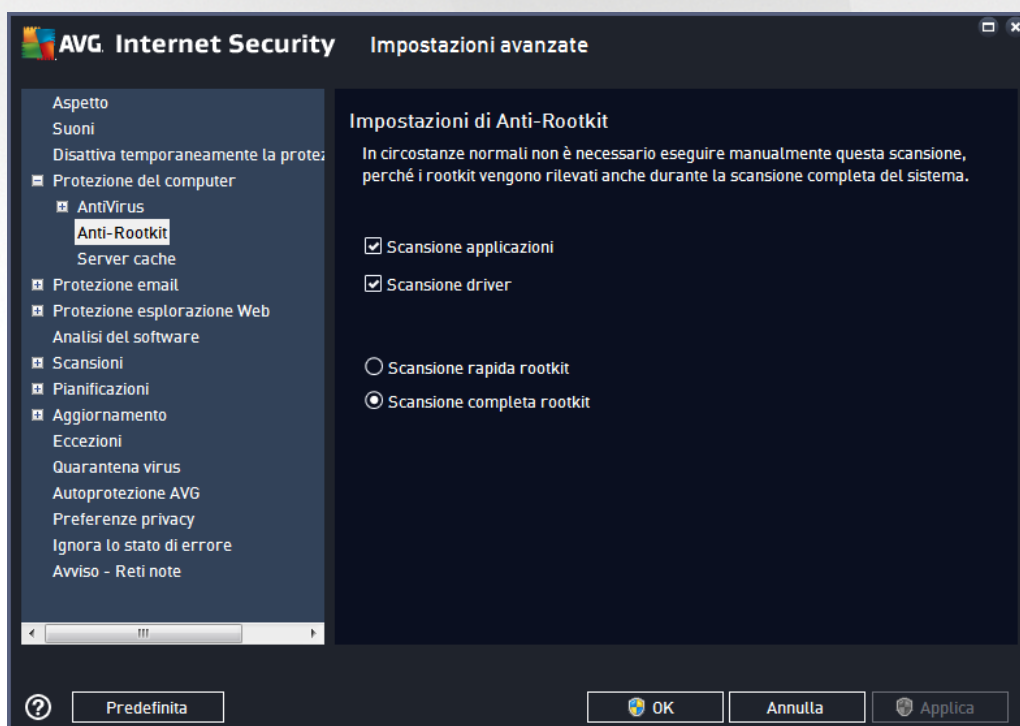
**Esegui la ricerca di rootkit nel computer** può essere avviato direttamente dalla finestra di dialogo [Opzioni di scansione](#) facendo clic sul pulsante **Esegui la ricerca di rootkit nel computer**. Verrà aperta una nuova finestra di dialogo **Scansione Anti-Rootkit in corso** che indica l'avanzamento della scansione avviata:





### Modifica della configurazione della scansione

È possibile modificare la configurazione della scansione Anti-Rootkit nella finestra di dialogo **Impostazioni di Anti-Rootkit** (accessibile tramite il collegamento *Impostazioni per la scansione* Esegui la ricerca di rootkit nel computer nella finestra di dialogo [Opzioni di scansione](#)). **Si consiglia di mantenere le impostazioni predefinite e di modificarle solo se esiste un reale motivo per farlo.**



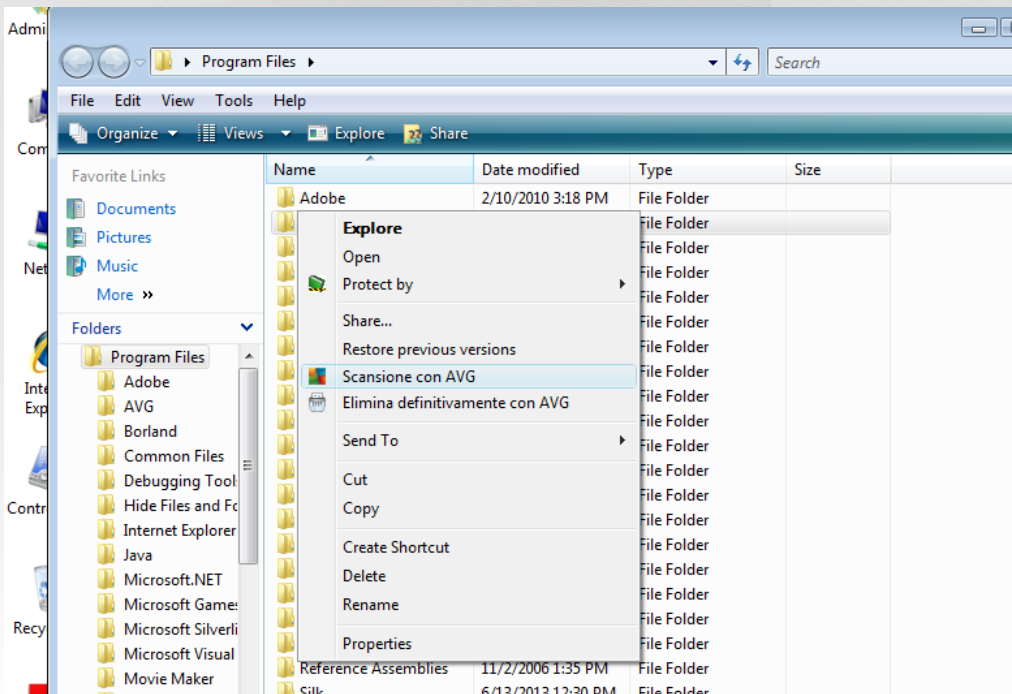
**Scansione applicazioni** e **Scansione driver** consentono di specificare in dettaglio gli elementi da includere nella scansione Anti-Rootkit. Queste impostazioni sono progettate per utenti esperti. Si consiglia di lasciare attivate tutte le opzioni. È inoltre possibile selezionare la modalità di scansione rootkit:



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

### 3.7.2. Scansione in Esplora risorse

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



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

### 3.7.3. Scansione dalla riga di comando

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

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

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





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

### 3.7.3.1. Sintassi del comando

La sintassi del comando è la seguente:

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

### 3.7.3.2. Parametri di scansione

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

Per eseguire la scansione, premere **Invio**. Durante la scansione è possibile arrestare il processo premendo **Ctrl+C** oppure **Ctrl+Pausa**.

### 3.7.3.3. Scansione CMD avviata dall'interfaccia grafica

Quando viene eseguita la modalità provvisoria di Windows, è inoltre possibile avviare la scansione da riga di comando dall'interfaccia utente grafica:



Nella modalità provvisoria la scansione verrà avviata dalla riga di comando. Questa finestra di dialogo consente solo di specificare i parametri di scansione nella comoda interfaccia grafica.



Innanzitutto, selezionare le aree del computer di cui eseguire la scansione. È possibile scegliere tra l'opzione predefinita **Scansione intero computer** o **Scansione file o cartelle**. La terza opzione, **Scansione rapida**, avvia una specifica scansione progettata per l'utilizzo nella modalità provvisoria che esamina tutte le aree critiche del computer necessarie per l'avvio.

Le impostazioni di scansione nella sezione successiva consentono di specificare parametri di scansione dettagliati. Tutte le impostazioni sono selezionate per impostazione predefinita. È consigliabile mantenerle selezionate e deselezionare un determinato parametro solo se necessario.

- **Ricerca "Applicazioni potenzialmente indesiderate"** - scansione per la ricerca degli spyware, in aggiunta ai virus
- **Esegui scansione flussi di dati alternativi (solo NTFS)** - scansione dei flussi di dati alternativi NTFS, una funzionalità di Windows che può essere utilizzata in modo improprio dai pirati informatici per nascondere dati, in particolare i codici dannosi
- **Correggi o rimuovi le infezioni automaticamente** - tutti i possibili rilevamenti verranno gestiti e saranno corretti o rimossi dal computer automaticamente
- **Scansione dei processi attivi** - scansione di processi e applicazioni caricati nella memoria del computer
- **Scansione del Registro di sistema** - scansione del Registro di sistema di Windows
- **Abilita controllo record di avvio principale (MBR)** - scansione della tabella delle partizioni e del settore di avvio

Infine, nella parte inferiore di questa finestra di dialogo è possibile specificare il nome del file e il tipo per il rapporto di scansione.

### **3.7.3.4. Parametri scansione CMD**

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

- `/?` Visualizza la Guida sull'argomento
- `/@` File di comando /nome file/
- `/ADS` Esegui scansione flussi di dati alternativi (*solo NTFS*)
- `/ARC` Esegui scansione su archivi
- `/ARCBOMBSW` Segnala file di archivio ricompresi
- `/ARCBOMBSW` Segnalazione delle bombe a decompressione (*archivi compressi più volte*)
- `/BOOT` Abilita controllo MBR/BOOT
- `/BOOTPATH` Avvia scansione rapida
- `/CLEAN` Pulisci automaticamente
- `/CLOUDCHECK` Ricerca di falsi positivi





- /COMP [Scansione intero computer](#)
- /COO Esegui scansione dei cookie
- /EXCLUDE Escludi percorso o file dalla scansione
- /EXT Esegui scansione su queste estensioni (*ad esempio EXT=EXE,DLL*)
- /FORCESHUTDOWN Arresto forzato del computer al completamento della scansione
- /HELP Visualizza la Guida sull'argomento
- /HEUR Utilizza analisi euristica
- /HIDDEN Segnala i file con estensione nascosta
- /IGNLOCKED Ignora file bloccati
- /INFECTABLEONLY Scansione dei soli file con estensioni infettabili
- /LOG Genera file risultati scansione
- /MACROW Segnala macro
- /NOBREAK Non consentire interruzione CTRL-BREAK
- /NOEXT Non eseguire scansione su queste estensioni (*ad esempio NOEXT=JPG*)
- /PRIORITY Impostazione della priorità per la scansione (*bassa, automatica, alta - vedere [Impostazioni avanzate / Scansioni](#)*)
- /PROC Scansione dei processi attivi
- /PUP Segnalazione delle applicazioni potenzialmente indesiderate
- /PUPEXT Segnalazione dei set potenziati di applicazioni potenzialmente indesiderate
- /PWDW Segnala file protetti da password
- /QT Controllo rapido
- /REG Scansione Registro di sistema
- /REPAPPEND Allega al file rapporto
- /REPOK Segnala file non infetti come OK
- /REPORT Rapporto sul file (*nome file*)
- /SCAN [Scansione file o cartelle](#) (*SCAN=percorso;percorso ad esempio /SCAN=C:\;D:\*)
- /SHUTDOWN Arresta computer al completamento della scansione

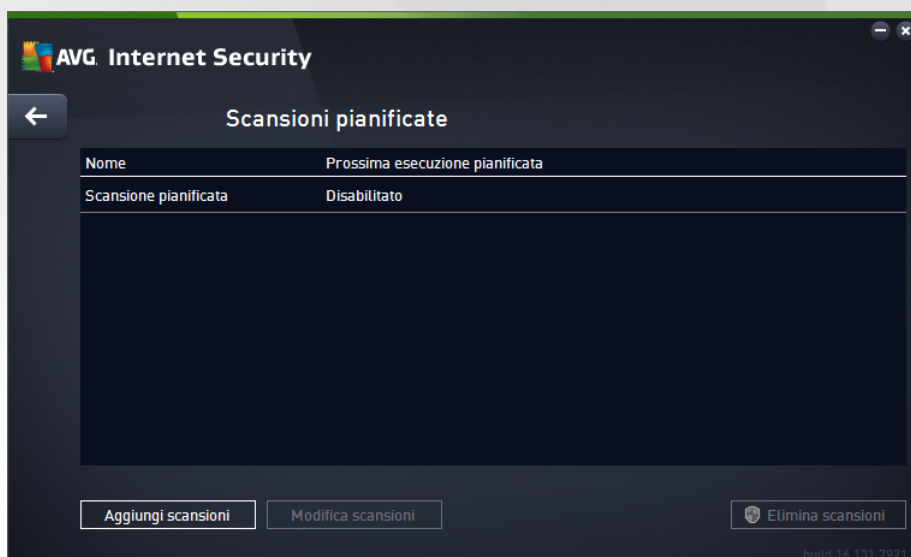


- /THOROUGHSCAN Attivazione della scansione completa
- /TRASH Sposta file infetti in [Quarantena virus](#)

### 3.7.4. Pianificazione di scansioni


**AVG Internet Security** consente di eseguire scansioni su richiesta (*ad esempio quando si sospetta che un'infezione sia stata trasferita nel computer*) oppure in base a una pianificazione. Si consiglia di eseguire le scansioni in base a una pianificazione: in questo modo ci si assicura che il computer sia protetto da possibili infezioni e non è necessario preoccuparsi dell'avvio della scansione. [Scansione intero computer](#) deve essere avviata regolarmente, almeno una volta alla settimana. Tuttavia, se possibile, avviare la scansione dell'intero computer ogni giorno, come impostato nella configurazione predefinita della pianificazione della scansione. Se il computer è sempre acceso, è possibile pianificare le scansioni fuori dagli orari di lavoro. Se il computer rimane a volte spento, è possibile pianificare l'esecuzione delle scansioni [all'avvio del computer, nel caso in cui l'attività non sia stata eseguita](#).

La pianificazione di scansione può essere creata / modificata nella finestra di dialogo **Scansioni pianificate** accessibile tramite il pulsante **Gestione scansioni pianificate** nella finestra di dialogo [Opzioni di scansione](#). Nella nuova finestra di dialogo **Scansione pianificata** è possibile visualizzare una panoramica completa di tutte le scansioni pianificate al momento:



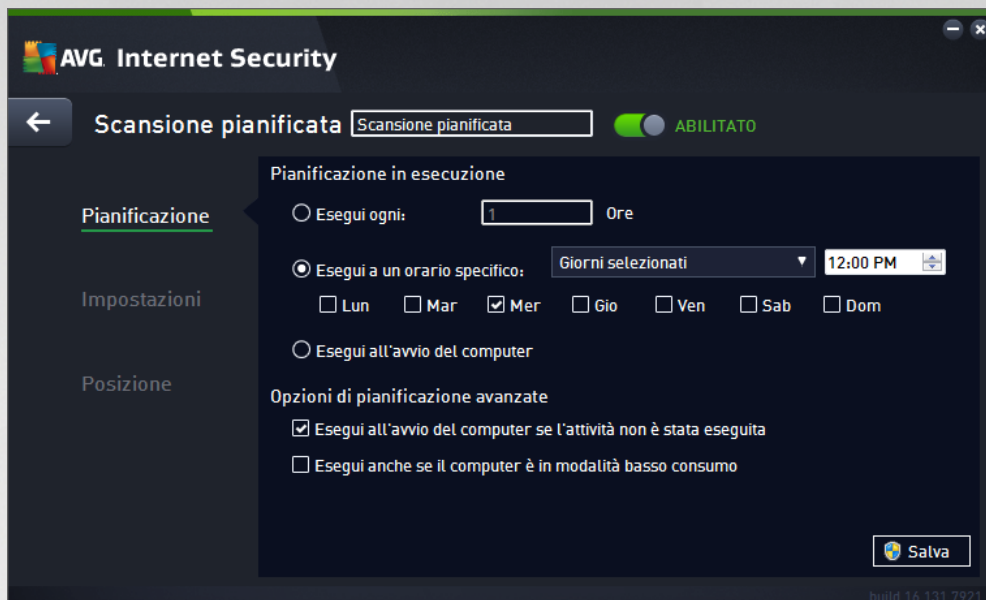
Nella finestra di dialogo è possibile specificare le scansioni personalizzate. Utilizzare il pulsante **Aggiungi scansione pianificata** per creare una nuova pianificazione di scansione personalizzata. È possibile modificare i parametri della scansione pianificata (*o configurare una nuova pianificazione*) in tre schede:

- [Pianificazione](#)
- [Impostazioni](#)
- [Posizione](#)

In ogni scheda è possibile impostare il pulsante "semaforo"  per disattivare temporaneamente il controllo pianificato e riattivarlo secondo le necessità.



### 3.7.4.1. Pianificazione



Nella parte superiore della scheda **Pianificazione** è disponibile il campo di testo in cui specificare il nome della pianificazione di scansione che si sta definendo attualmente. Denominare le scansioni assegnando sempre nomi brevi, descrittivi e appropriati per poterle riconoscere più facilmente in futuro. Ad esempio, non è appropriato denominare una scansione "Nuova scansione" o "Scansione personale" poiché questi nomi non fanno riferimento agli elementi sottoposti a scansione. Un esempio di un buon nome descrittivo potrebbe essere "Scansione aree di sistema" e così via.


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

- **Pianificazione esecuzione** - consente di specificare gli intervalli di tempo per l'avvio della nuova scansione pianificata. È possibile definire l'ora tramite l'avvio ripetuto della scansione dopo un certo periodo di tempo (*Esegui ogni...*), specificando data e ora esatte (*Esegui a un orario specifico*) oppure definendo un evento a cui dovrà essere associato l'avvio della scansione (*Esegui all'avvio del computer*).
- **Opzioni di pianificazione avanzate** - questa sezione consente di definire le circostanze in cui deve essere avviata o non avviata la scansione se il computer si trova in modalità basso consumo oppure se è completamente spento. Quando la scansione pianificata viene avviata all'ora specificata, l'utente ne viene informato tramite una finestra popup visualizzata sopra l'icona di AVG nell'area di notifica. Nell'area di notifica viene quindi visualizzata una nuova icona di AVG (completamente colorata e con una luce lampeggiante) che segnala che è in corso una scansione pianificata. Fare clic con il pulsante destro del mouse sull'icona AVG della scansione in esecuzione per aprire un menu di scelta rapida in cui è possibile decidere se sospendere o arrestare la scansione in esecuzione, nonché modificarne la priorità.

#### Controlli nella finestra di dialogo

- **Salva** - consente di salvare tutte le modifiche eseguite su questa scheda o su un'altra scheda della finestra di dialogo e di tornare alla panoramica delle [scansioni pianificate](#). Pertanto, se si desidera configurare i parametri di controllo di tutte le schede, selezionare il pulsante per salvarli solo dopo aver specificato tutti i requisiti desiderati.



-  - usare la freccia verde nella parte superiore sinistra della finestra di dialogo per tornare alla panoramica delle [scansioni pianificate](#).

### 3.7.4.2. Impostazioni



Nella parte superiore della scheda **Impostazioni** è possibile trovare il campo di testo in cui specificare il nome della pianificazione di scansione che si sta definendo attualmente. Denominare le scansioni assegnando sempre nomi brevi, descrittivi e appropriati per poterle riconoscere più facilmente in futuro. Ad esempio, non è appropriato denominare una scansione "Nuova scansione" o "Scansione personale" poiché questi nomi non fanno riferimento agli elementi sottoposti a scansione. Un esempio di un buon nome descrittivo potrebbe essere "Scansione aree di sistema" e così via.

Nella scheda **Impostazioni** è contenuto un elenco di parametri di scansione che possono essere attivati/disattivati facoltativamente. **A meno che ci sia una ragione valida per modificare le impostazioni, si consiglia di mantenere la configurazione predefinita:**

- **Correggi/Rimuovi infezioni da virus senza richiedere conferma** (attivata per impostazione predefinita): se viene identificato un virus durante la scansione può essere corretto automaticamente se è disponibile una soluzione. Se il file infetto non può essere corretto automaticamente, l'oggetto infetto verrà spostato in [Quarantena virus](#).
- **Segnala applicazioni potenzialmente indesiderate e minacce spyware** (attivata per impostazione predefinita): selezionare questa casella di controllo per attivare la scansione per ricercare spyware e virus. Gli spyware rappresentano una categoria di malware anomala: anche se solitamente costituiscono un rischio per la sicurezza, alcuni di questi programmi possono essere installati intenzionalmente. Si consiglia di mantenere questa funzionalità attivata in quanto consente di aumentare la protezione del computer.
- **Segnala set potenziati di applicazioni potenzialmente indesiderate** (disattivata per impostazione predefinita): selezionare per rilevare pacchetti estesi di spyware, ovvero programmi perfettamente normali e innocui al momento dell'acquisto diretto presso il produttore, ma utilizzabili a scopi dannosi successivamente. Si tratta di una precauzione aggiuntiva che aumenta ulteriormente la protezione del computer, ma che potrebbe bloccare programmi legittimi, pertanto l'opzione è disattivata per impostazione predefinita.

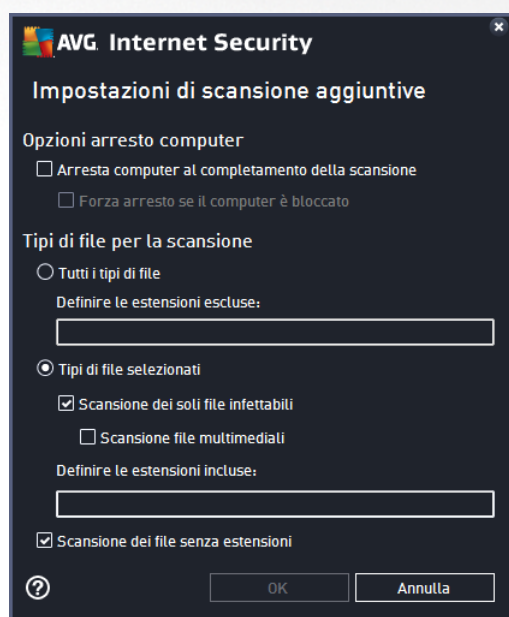




- **Scansione dei cookie di rilevamento** (disattivata per impostazione predefinita): questo parametro stabilisce che i cookie devono essere rilevati durante la scansione (i cookie HTTP vengono utilizzati per autenticare, rilevare e mantenere informazioni specifiche sugli utenti, quali i siti preferiti o il contenuto dei carrelli elettronici).
- **Scansione all'interno degli archivi** (disattivata per impostazione predefinita): questo parametro stabilisce che la scansione deve controllare tutti i file anche se inclusi all'interno di un tipo di archivio, quale ZIP, RAR e così via.
- **Usa analisi euristiche** (attivata per impostazione predefinita): l'analisi euristica (emulazione dinamica delle istruzioni dell'oggetto sottoposto a scansione in un ambiente informatico virtuale) sarà uno dei metodi utilizzati per il rilevamento di virus durante la scansione.
- **Scansione ambiente di sistema** (attivata per impostazione predefinita): la scansione verrà eseguita anche sulle aree di sistema del computer.
- **Attiva scansione completa** (disattivata per impostazione predefinita): in situazioni specifiche (ad esempio se si sospetta che il computer sia stato infettato) per maggiore sicurezza è possibile selezionare questa opzione per attivare gli algoritmi di scansione più completi che esamineranno anche le aree del computer che difficilmente vengono infettate. Tenere presente tuttavia che questo metodo è piuttosto dispendioso in termini di tempo.
- **Ricerca di rootkit** (attivata per impostazione predefinita): la scansione Anti-Rootkit ricerca sul computer la presenza di eventuali rootkit (programmi e tecnologie in grado di coprire l'attività dei malware nel computer). Se viene rilevato un rootkit, ciò non significa necessariamente che il computer sia infetto. In alcuni casi, specifici driver o sezioni di applicazioni regolari possono venire rilevati erroneamente come rootkit.

### Impostazioni di scansione aggiuntive

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





- **Opzioni arresto computer** - consente di decidere se il computer deve essere arrestato automaticamente al termine del processo di scansione. Dopo aver confermato questa opzione (*Arresta computer al completamento della scansione*), viene attivata una nuova opzione che consente l'arresto del computer anche se è correntemente bloccato (*Forza arresto se il computer è bloccato*).
- **Tipi di file per la scansione** - specificare se si desidera sottoporre a scansione:
  - **Tutti i tipi di file** con l'opzione per definire le eccezioni fornendo un elenco di estensioni di file separate da virgola da non sottoporre a scansione.
  - **Tipi di file selezionati** - è possibile specificare che si desidera sottoporre a scansione solo i file potenzialmente infettabili (*i file che non possono essere infettati non verranno sottoposti a scansione, ad esempio alcuni file di testo normale o altri file non eseguibili*), inclusi i file multimediali (*file video e audio; se non si seleziona questa casella, il tempo di scansione risulterà ulteriormente ridotto, poiché questi file sono spesso di grandi dimensioni e non facilmente infettabili da un virus*). Anche in questo caso, è possibile specificare tramite le estensioni quali file devono essere sempre sottoposti a scansione.
  - Facoltativamente, è possibile effettuare la **Scansione dei file senza estensioni**: questa opzione è attivata per impostazione predefinita e si consiglia di non modificarla a meno che non si abbiano motivi validi per farlo. I file senza estensione sono piuttosto sospetti e devono essere sempre sottoposti a scansione.

### Regola la velocità di completamento della scansione

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

### Imposta rapporti di scansione aggiuntivi

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



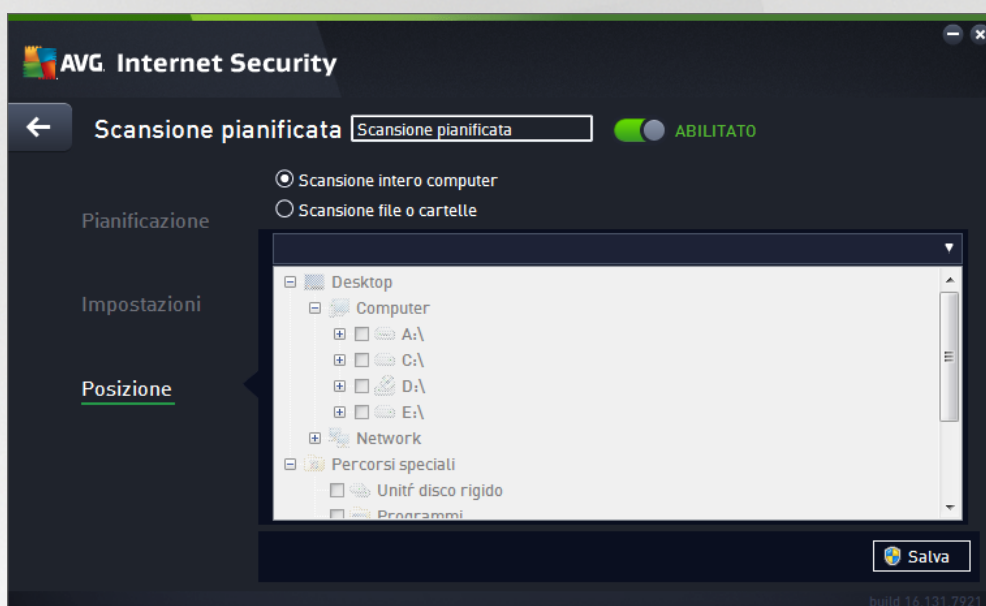




### Controlli nella finestra di dialogo

- **Salva** - consente di salvare tutte le modifiche eseguite su questa scheda o su un'altra scheda della finestra di dialogo e di tornare alla panoramica delle [scansioni pianificate](#). Pertanto, se si desidera configurare i parametri di controllo di tutte le schede, selezionare il pulsante per salvarli solo dopo aver specificato tutti i requisiti desiderati.
- **←** - usare la freccia verde nella parte superiore sinistra della finestra di dialogo per tornare alla panoramica delle [scansioni pianificate](#).

### 3.7.4.3. Posizione



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

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

- **Dischi rigidi locali** - tutti i dischi rigidi del computer
- **Programmi**
  - C:\Programmi\
  - *nella versione a 64 bit* C:\Programmi (x86)



- **Cartella Documenti**

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

- **Documenti condivisi**


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

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

- **Altro**

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

### Controlli nella finestra di dialogo

- **Salva** - consente di salvare tutte le modifiche eseguite su questa scheda o su un'altra scheda della finestra di dialogo e di tornare alla panoramica delle [scansioni pianificate](#). Pertanto, se si desidera configurare i parametri di controllo di tutte le schede, selezionare il pulsante per salvarli solo dopo aver specificato tutti i requisiti desiderati.
-  - usare la freccia verde nella parte superiore sinistra della finestra di dialogo per tornare alla panoramica delle [scansioni pianificate](#).





### 3.7.5. Risultati scansione

Nome	Ora di inizio	Ora di fine	Oggetti contro...	Infezioni	Alta
Scansione Antirookit	11/1/2016, 5:17	11/1/2016, 5:17	31502	0	0
Scansione intero computer	11/1/2016, 5:17	11/1/2016, 5:17	5039	0	0

Nella finestra di dialogo **Panoramica risultati di scansione** è contenuto l'elenco dei risultati di tutte le scansioni eseguite in precedenza. Il grafico fornisce le seguenti informazioni su ciascun risultato della scansione:

- **Icona** - nella prima colonna è visualizzata un'icona informativa che descrive lo stato della scansione:
  - Nessuna infezione rilevata, scansione completata
  - Nessuna infezione rilevata, scansione interrotta prima del completamento
  - Infezioni rilevate e non corrette, scansione completata
  - Infezioni rilevate e non corrette, scansione interrotta prima del completamento
  - Infezioni rilevate e corrette o rimosse, scansione completata
  - Infezioni rilevate e corrette o rimosse, scansione interrotta prima del completamento
- **Nome** - in questa colonna viene visualizzato il nome della rispettiva scansione. Si tratta di una delle due [scansioni predefinite](#) oppure della [scansione pianificata](#) dall'utente.
- **Ora di inizio** - indica la data e l'ora esatte di avvio della scansione.
- **Ora di fine** - indica la data e l'ora esatte in cui la scansione è stata completata, sospesa o interrotta.
- **Oggetti controllati** - indica il numero totale di tutti gli oggetti sottoposti a scansioni.
- **Infezioni** - indica il numero di infezioni rilevate totali/rimosse.
- **Alto / Medio / Basso** - le seguenti colonne indicano il numero di infezioni rilevate con livello di gravità alto, medio o basso rispettivamente.



- **Rootkit** - indica il numero totale di [rootkit](#) rilevati durante la scansione.

### Comandi della finestra di dialogo

**Visualizza dettagli** - fare clic sul pulsante per visualizzare [informazioni dettagliate su una scansione selezionata](#) (evidenziata nel grafico sopra).

**Elimina risultati** - fare clic sul pulsante per rimuovere un risultato della scansione selezionato nel grafico.

← - usare la freccia verde nella parte superiore sinistra della finestra di dialogo per tornare all'[interfaccia utente principale](#) con la panoramica dei componenti.

### 3.7.6. Dettagli di Risultati scansione

Per aprire una panoramica delle informazioni dettagliate su un risultato scansione selezionato, fare clic sul pulsante **Visualizza dettagli** disponibile nella finestra di dialogo [Panoramica risultati di scansione](#). Si verrà reindirizzati alla stessa interfaccia che descrive dettagliatamente le informazioni sui rispettivi risultati della scansione. Le informazioni sono divise in tre schede:

- **Riepilogo**: questa scheda fornisce informazioni di base sulla scansione (se è stata completata, se sono state rilevate minacce e l'operazione che è stata eseguita su di esse).
- **Dettagli**: in questa scheda vengono visualizzate tutte le informazioni sulla scansione, inclusi i dettagli relativi a eventuali minacce rilevate. Esporta panoramica nel file consente di salvarla come file .csv.
- **Rilevamenti**: questa scheda viene visualizzata solo se sono state rilevate minacce durante la scansione e fornisce informazioni dettagliate sulle minacce.

● **Livello di gravità informazioni**: informazioni o avvisi, non minacce effettive. In genere, documenti che contengono macro, documenti o archivi protetti da password, file bloccati e così via.

●● **Livello di gravità medio**: PUP (programmi potenzialmente indesiderati, *come ad esempio adware*) o cookie di rilevamento

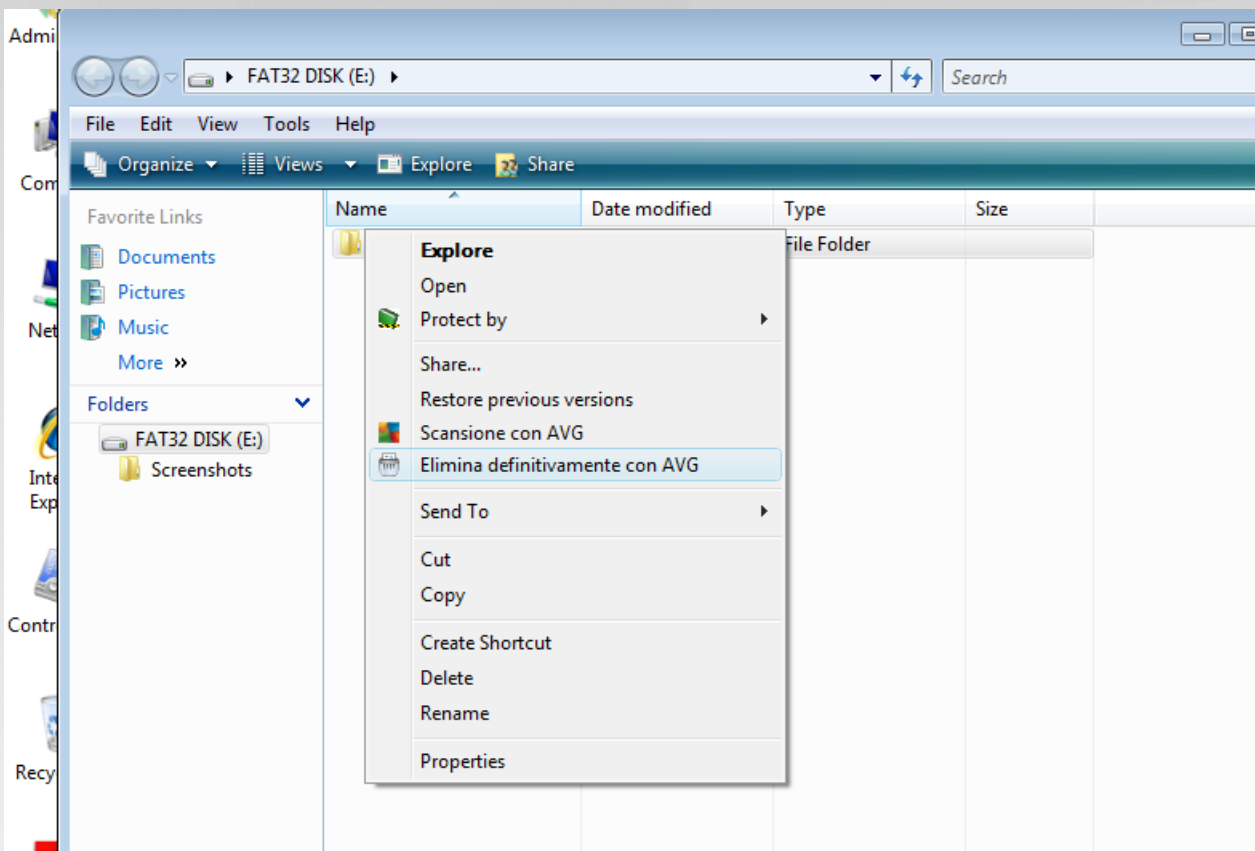
●●● **Livello di gravità alto**: minacce gravi come virus, trojan, exploit e così via. Anche oggetti individuati dal metodo di rilevamento dell'analisi euristica, ovvero minacce non ancora descritte nel database dei virus.

### 3.8. AVG File Shredder

**AVG File Shredder** è stato creato per eliminare i file in tutta sicurezza, ovvero senza possibilità di ripristinarli, neppure con strumenti software avanzati specifici per questo scopo.

Per eliminare definitivamente un file o una cartella, fare clic con il pulsante destro del mouse su un file manager (*Esplora risorse, Total Commander e così via*) e selezionare **Elimina definitivamente con AVG** dal menu di scelta rapida. Anche i file presenti nel Cestino possono essere eliminati definitivamente. Se non è possibile eliminare in modo definitivo e affidabile un file specifico in un percorso specifico (*ad esempio, in un CD-ROM*), verrà visualizzata una notifica o l'opzione nel menu di scelta rapida non sarà disponibile.





**È importante tenere presente che dopo aver eliminato un file in modo definitivo, non sarà possibile recuperarlo.**

### 3.9. Quarantena virus

**Quarantena virus** è un ambiente protetto per la gestione degli oggetti sospetti o infetti rilevati durante i controlli AVG. Se durante la scansione viene rilevato un oggetto infetto e AVG non è in grado di ripararlo automaticamente, viene richiesto quale operazione eseguire sull'oggetto sospetto. La soluzione consigliata è spostare l'oggetto in **Quarantena virus** per un'ulteriore elaborazione. Lo scopo principale di **Quarantena virus** è quello di conservare ciascun file eliminato per un periodo di tempo sufficiente ad accertare che il file non sia più necessario nella posizione originale. Se l'assenza del file dovesse causare problemi, è possibile inviare il file in questione per l'analisi o ripristinarlo nella posizione originale.

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

- **Data aggiunta** - data e ora del rilevamento e dell'inserimento in Quarantena virus del file sospetto.
- **Minaccia** - se è stato installato il componente [Analisi del software](#) in **AVG Internet Security**, questa sezione fornirà l'identificazione grafica della gravità del rilevamento: dal livello più sicuro (*tre punti verdi*) al più pericoloso (*tre punti rossi*). Saranno inoltre disponibili informazioni sul tipo di infezione e sulla posizione originale. Il collegamento *Ulteriori informazioni* visualizza una pagina con informazioni dettagliate sulla minaccia rilevata, tratte dall'[enciclopedia dei virus online](#).
- **Origine** - specifica il componente di **AVG Internet Security** da cui è stata rilevata la rispettiva minaccia.



- **Notifiche** - in alcune situazioni, in questa colonna possono essere visualizzate note con commenti dettagliati sulla rispettiva minaccia rilevata.

### Pulsanti di controllo

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

- **Ripristina** - consente di ripristinare il file infetto nella posizione originale sul disco.
- **Ripristina come** - sposta il file infetto nella cartella selezionata.
- **Invia per analisi** - il pulsante è attivo solo quando si evidenzia un oggetto nell'elenco dei rilevamenti superiore. In tal caso, è possibile inviare il rilevamento selezionato ai Virus Lab di AVG per un'ulteriore analisi dettagliata. Tenere presente che questa funzionalità deve essere utilizzata principalmente per inviare i falsi positivi, ovvero i file rilevati da AVG come infetti o sospetti, ma ritenuti innocui dall'utente.
- **Dettagli** - per informazioni dettagliate sulla minaccia specifica spostata in **Quarantena virus**, evidenziare l'elemento selezionato nell'elenco e fare clic sul pulsante **Dettagli** per aprire una nuova finestra di dialogo con la descrizione della minaccia rilevata.
- **Elimina** - consente di rimuovere definitivamente il file infetto da **Quarantena virus**.
- **Svuota Quarantena** - elimina completamente tutto il contenuto di **Quarantena virus**. I file rimossi da **Quarantena virus** vengono eliminati in modo definitivo dal disco (*non vengono spostati nel Cestino*).

## 3.10. Cronologia

La sezione **Cronologia** include informazioni su tutti gli eventi precedenti (*ad esempio aggiornamenti, scansioni, rilevamenti e così via*) e i rapporti relativi a tali eventi. Questa sezione è accessibile dall'[interfaccia utente principale](#) tramite la voce **Opzioni / Cronologia**. Inoltre, la cronologia di tutti gli eventi registrati è suddivisa nelle seguenti parti:

- [Risultati scansione](#)
- [Risultati di Resident Shield](#)
- [Risultati di Protezione email](#)
- [Risultati di Online Shield](#)
- [Cronologia eventi](#)
- [Log Firewall](#)




### 3.10.1. Risultati scansione




La finestra di dialogo **Panoramica risultati di scansione** è accessibile tramite la voce **Opzioni / Cronologia / Risultati scansione** nel menu di spostamento superiore della finestra principale di **AVG Internet Security**. Nella finestra di dialogo è contenuto l'elenco di tutte le scansioni avviate in precedenza e le informazioni sui relativi risultati:

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

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

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

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

Ciascuna icona può essere intera o suddivisa in due parti: l'icona intera indica una scansione completata correttamente, l'icona suddivisa in due indica una scansione annullata o interrotta.

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


- **Ora di inizio** - data e ora di avvio della scansione
- **Ora di fine** - data e ora del completamento della scansione
- **Oggetti controllati** - numero di oggetti controllati durante la scansione



- **Infezioni** - numero delle infezioni da virus rilevate / rimosse
- **Alto / Medio** - queste colonne indicano il numero di infezioni totali o rimosse con livello di gravità alto o medio rispettivamente
- **Informazioni** - informazioni relative all'andamento e al risultato della scansione (*in genere in relazione alla finalizzazione o all'interruzione*)
- **Rootkit** - numero di [rootkit](#) rilevati

### Pulsanti di controllo

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

- **Visualizza dettagli** - selezionare questa opzione per accedere alla finestra di dialogo [Risultati scansione](#) e visualizzare dati dettagliati relativi alla scansione selezionata
- **Elimina risultato** - selezionare questa opzione per rimuovere la voce selezionata dalla panoramica dei risultati di scansione
-  - per tornare alla [finestra di dialogo principale di AVG predefinita \(panoramica dei componenti\)](#), utilizzare la freccia nell'angolo superiore sinistro di questa finestra di dialogo

## 3.10.2. Risultati di Resident Shield

Il servizio **Resident Shield** fa parte del componente [Computer](#) ed esegue la scansione dei file mentre vengono copiati, aperti o salvati. Quando viene rilevato un virus o altra minaccia, l'utente viene avvisato immediatamente tramite la successiva finestra di dialogo:



In questa finestra di dialogo di avviso sono disponibili informazioni sull'oggetto rilevato e giudicato infetto (*Minaccia*) e alcuni dati descrittivi sull'infezione riconosciuta (*Descrizione*). Il collegamento *Ulteriori informazioni* visualizza una pagina con informazioni dettagliate sulla minaccia rilevata, tratte dall'[enciclopedia dei virus online](#) (se note). Nella finestra di dialogo verrà inoltre visualizzata una panoramica delle soluzioni disponibili per gestire la minaccia rilevata. Una delle alternative verrà contrassegnata come consigliata: **Proteggimi (scelta consigliata)**. **Se possibile, si consiglia di attenersi sempre a questa opzione.**





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

Nella parte inferiore della finestra di dialogo è possibile trovare il collegamento **Mostra dettagli**. Fare clic sul pulsante per aprire una nuova finestra con informazioni dettagliate sul processo in esecuzione durante il rilevamento dell'infezione e i dati identificativi del processo.

Un elenco di tutti i rilevamenti di Resident Shield è disponibile per una panoramica all'interno della finestra di dialogo **Rilevamento Resident Shield**. Questa finestra di dialogo è accessibile tramite la voce **Opzioni / Cronologia / Rilevamento Resident Shield** nel menu di spostamento superiore della [finestra principale](#) di **AVG Internet Security**. Nella finestra di dialogo è disponibile una panoramica di oggetti rilevati da Resident Shield, classificati come pericolosi e corretti o spostati in [Quarantena virus](#).




Per ogni oggetto rilevato vengono fornite le seguenti informazioni:

- **Nome della minaccia** - descrizione (possibilmente anche il nome) dell'oggetto rilevato e relativa posizione. Il collegamento *Ulteriori informazioni* visualizza una pagina con informazioni dettagliate sulla minaccia rilevata, tratte dall'[enciclopedia dei virus online](#).
- **Stato** - azione eseguita sull'oggetto rilevato
- **Ora di rilevamento** - data e ora in cui la minaccia è stata rilevata e bloccata
- **Tipo di oggetto** - tipo di oggetto rilevato
- **Processo** - operazione eseguita per richiamare e rilevare l'oggetto potenzialmente pericoloso

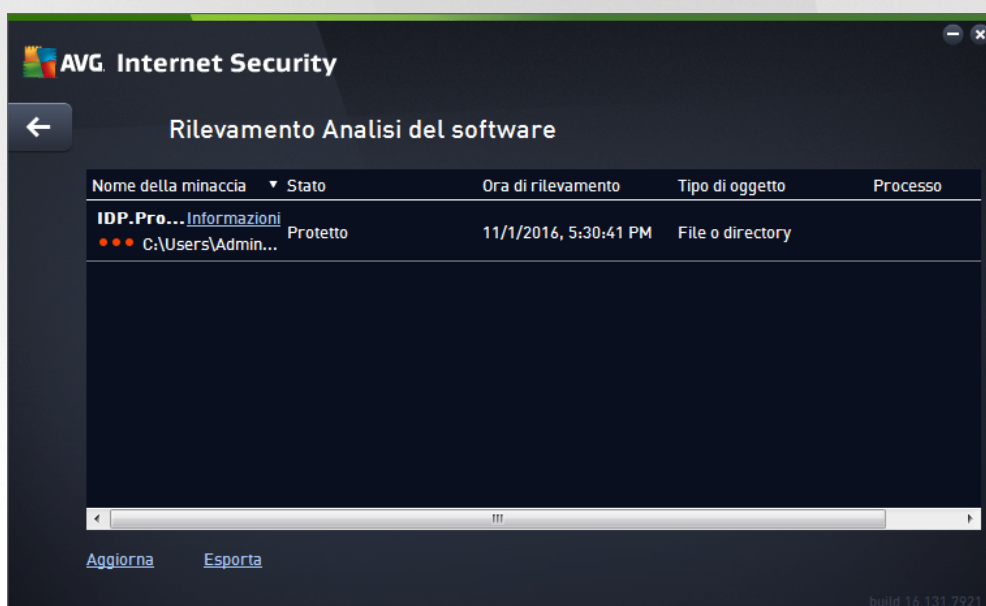


### Pulsanti di controllo

- **Aggiorna** - consente di aggiornare l'elenco dei rilevamenti effettuati da **Online Shield**
- **Esporta** - consente di esportare l'intero elenco di oggetti rilevati in un file
- **Rimuovi voci selezionate** - nell'elenco è possibile evidenziare i record selezionati e utilizzare questo pulsante per eliminare solo tali elementi
- **Rimuovi tutte le minacce** - fare clic su questo pulsante per eliminare tutti i record elencati in questa finestra di dialogo
-  - per tornare alla [finestra di dialogo principale di AVG predefinita \(panoramica dei componenti\)](#), utilizzare la freccia nell'angolo superiore sinistro di questa finestra di dialogo

### 3.10.3. Risultati di Identity Protection

La finestra di dialogo **Risultati di Analisi del software** è accessibile tramite la voce **Opzioni / Cronologia / Risultati di Analisi del software** nel menu di spostamento superiore della finestra principale di **AVG Internet Security**.



La finestra di dialogo fornisce un elenco di tutti i rilevamenti effettuati dal componente [Analisi del software](#). Per ogni oggetto rilevato vengono fornite le seguenti informazioni:

- **Nome della minaccia** - descrizione (possibilmente anche il nome) dell'oggetto rilevato e relativa posizione. Il collegamento *Ulteriori informazioni* visualizza una pagina con informazioni dettagliate sulla minaccia rilevata, tratte dall'[enciclopedia dei virus online](#).
- **Stato** - azione eseguita sull'oggetto rilevato
- **Ora di rilevamento** - data e ora in cui la minaccia è stata rilevata e bloccata
- **Tipo di oggetto** - tipo di oggetto rilevato






- **Processo** - operazione eseguita per richiamare e rilevare l'oggetto potenzialmente pericoloso

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

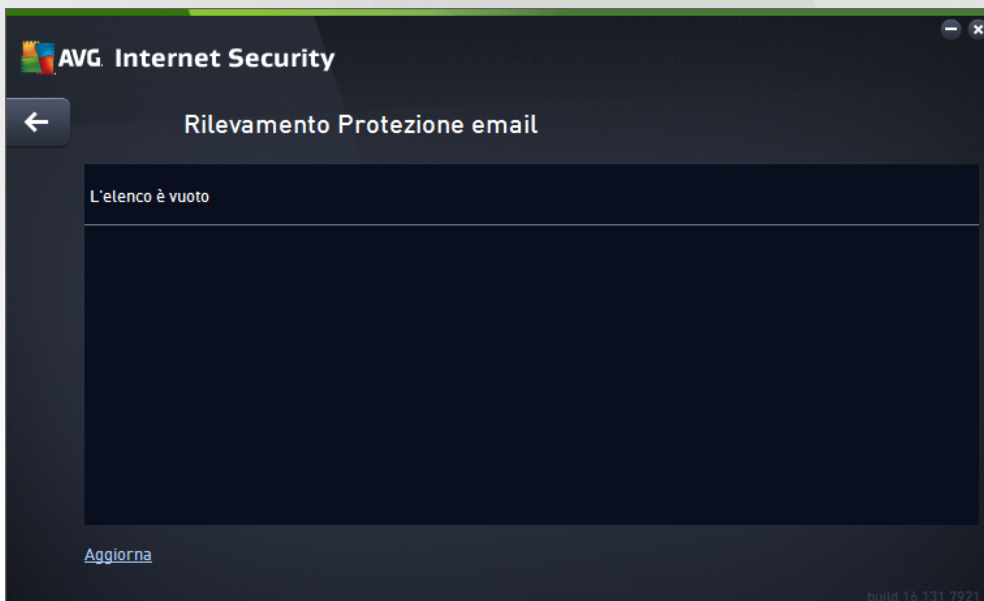
### Pulsanti di controllo

I pulsanti di controllo disponibili nell'interfaccia **Risultati di Analisi del software** sono i seguenti:

- **Aggiorna elenco** - consente di aggiornare l'elenco delle minacce rilevate
-  - per tornare alla [finestra di dialogo principale predefinita di AVG](#) (*panoramica dei componenti*), utilizzare la freccia nell'angolo superiore sinistro di questa finestra di dialogo

## 3.10.4. Risultati di Protezione email

La finestra di dialogo **Risultati di Protezione email** è accessibile tramite la voce **Opzioni / Cronologia / Risultati di Protezione email** nel menu di spostamento superiore della finestra principale di **AVG Internet Security**.



La finestra di dialogo fornisce un elenco di tutti i rilevamenti effettuati dal componente [Scansione Email](#). Per ogni oggetto rilevato vengono fornite le seguenti informazioni:

- **Nome rilevamento** - descrizione (*possibilmente anche il nome*) dell'oggetto rilevato e la relativa posizione
- **Risultato** - azione eseguita sull'oggetto rilevato
- **Ora di rilevamento** - data e ora in cui l'oggetto sospetto è stato rilevato
- **Tipo di oggetto** - tipo di oggetto rilevato




- **Processo** - operazione eseguita per richiamare e rilevare l'oggetto potenzialmente pericoloso

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

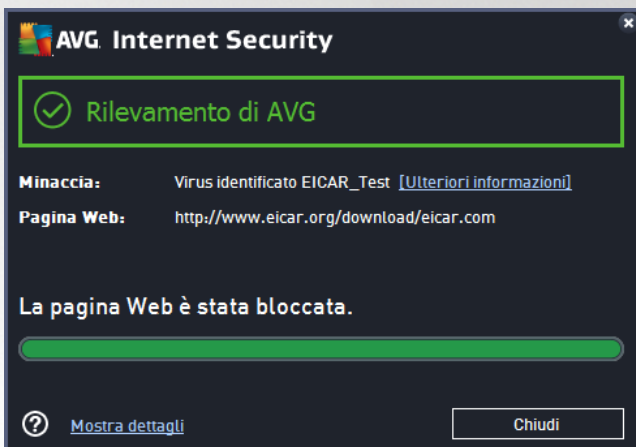
### Pulsanti di controllo

I pulsanti di controllo disponibili nell'interfaccia di **Rilevamento Scansione Email** sono i seguenti:

- **Aggiorna elenco** - consente di aggiornare l'elenco delle minacce rilevate
-  - per tornare alla [finestra di dialogo principale di AVG predefinita \(panoramica dei componenti\)](#), utilizzare la freccia nell'angolo superiore sinistro di questa finestra di dialogo

## 3.10.5. Risultati di Online Shield

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



In questa finestra di dialogo di avviso sono disponibili informazioni sull'oggetto rilevato e giudicato infetto (**Minaccia**) e alcuni dati descrittivi sull'infezione riconosciuta (**Nome oggetto**). Selezionando il collegamento **Ulteriori informazioni** si verrà reindirizzati all'[enciclopedia dei virus online](#) in cui è possibile trovare informazioni dettagliate sull'infezione rilevata (se note). La finestra di dialogo fornisce i seguenti elementi di controllo:

- **Mostra dettagli** - fare clic sul collegamento per aprire una nuova finestra popup con informazioni sul processo in esecuzione durante il rilevamento dell'infezione e i dati identificativi del processo.
- **Chiudi** - fare clic sul pulsante per chiudere la finestra di dialogo di avviso.

La pagina Web sospetta non verrà aperta e il rilevamento della minaccia verrà registrato nell'elenco **Rilevamenti di Online Shield**. Questa panoramica di minacce rilevate è accessibile tramite la voce **Opzioni / Cronologia / Rilevamenti di Online Shield** nel menu di spostamento superiore della finestra principale di **AVG Internet Security**.






Per ogni oggetto rilevato vengono fornite le seguenti informazioni:

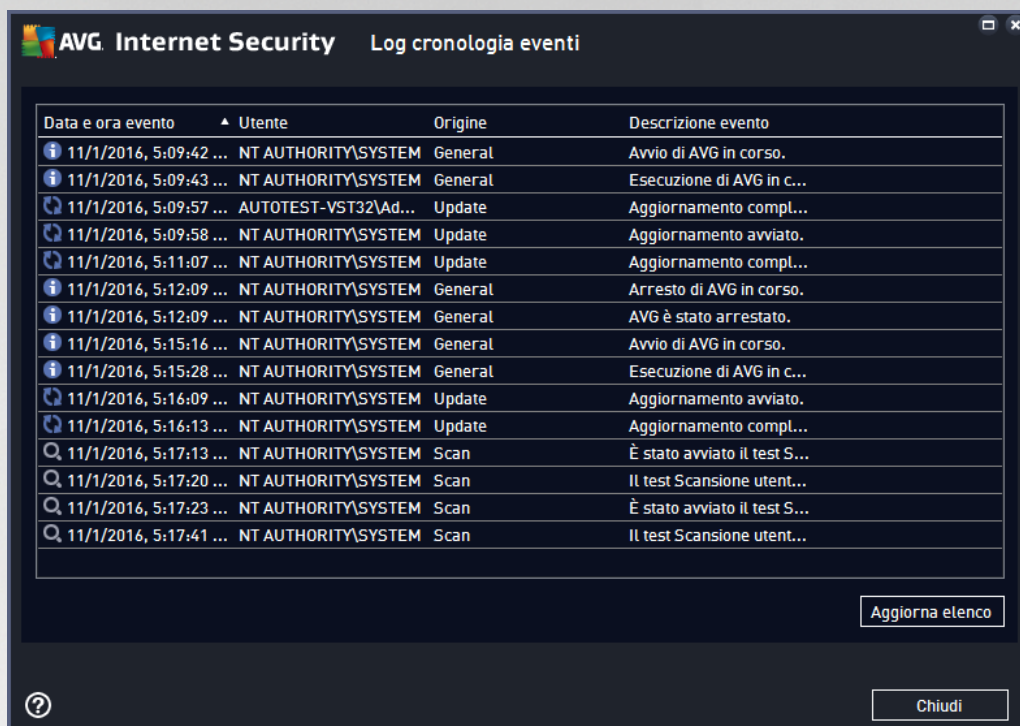
- **Nome della minaccia** - descrizione (possibilmente anche il nome) dell'oggetto rilevato e relativa origine (pagina Web). Il collegamento *Ulteriori informazioni* visualizza una pagina con informazioni dettagliate sulla minaccia rilevata, tratte dall'[enciclopedia dei virus online](#).
- **Stato** - azione eseguita sull'oggetto rilevato
- **Ora di rilevamento** - data e ora in cui la minaccia è stata rilevata e bloccata
- **Tipo di oggetto** - tipo di oggetto rilevato

#### Pulsanti di controllo

- **Aggiorna** - consente di aggiornare l'elenco dei rilevamenti effettuati da **Online Shield**
- **Esporta** - consente di esportare l'intero elenco di oggetti rilevati in un file
-  - per tornare alla [finestra di dialogo principale di AVG predefinita \(panoramica dei componenti\)](#), utilizzare la freccia nell'angolo superiore sinistro di questa finestra di dialogo



### 3.10.6. Cronologia eventi



La finestra di dialogo **Cronologia eventi** è accessibile tramite la voce **Opzioni / Cronologia / Cronologia eventi** nel menu di spostamento superiore della finestra principale di **AVG Internet Security**. In questa finestra di dialogo è possibile trovare un riepilogo di importanti eventi che si sono verificati durante l'attività di **AVG Internet Security**. La finestra di dialogo fornisce i record dei seguenti tipi di eventi: informazioni sugli aggiornamenti dell'applicazione AVG, informazioni sull'inizio, la fine o l'arresto della scansione (*inclusi i controlli eseguiti automaticamente*), informazioni sugli eventi connessi al rilevamento di un virus (*tramite la protezione permanente o la [scansione](#)*) inclusa la relativa posizione e altri eventi importanti.

Per ciascun evento vengono indicate le seguenti informazioni:

- **Data e ora evento** indica la data e l'ora esatte in cui si è verificato l'evento.
- **Utente** indica il nome dell'utente connesso nel momento in cui si è verificato l'evento.
- **Origine** fornisce informazioni sul componente di origine o altra parte del sistema AVG che ha attivato l'evento.
- **Descrizione evento** presenta un breve riepilogo dell'evento che si è verificato.

#### Pulsanti di controllo

- **Aggiorna elenco** - fare clic su questo pulsante per aggiornare tutte le voci incluse nell'elenco degli eventi
- **Chiudi** - fare clic sul pulsante per tornare alla finestra principale di **AVG Internet Security**



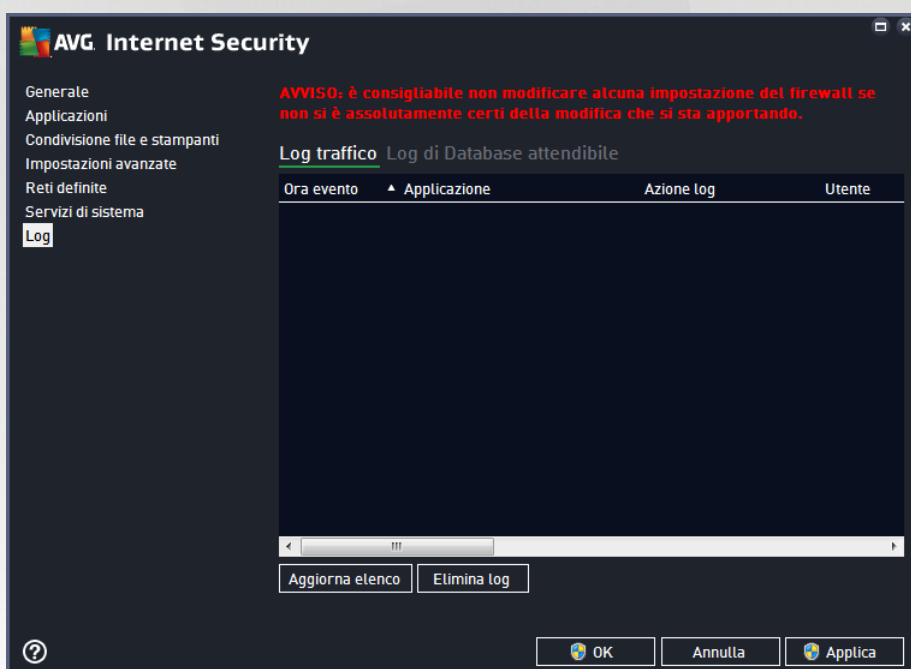


### 3.10.7. Log Firewall

**Questa finestra di dialogo è utilizzata per una configurazione avanzata. È consigliabile non modificare le impostazioni se non si è assolutamente sicuri che sia necessario.**

La finestra di dialogo **Log** consente di visualizzare l'elenco di tutte le azioni e gli eventi registrati di Firewall con una descrizione dettagliata dei parametri rilevanti mostrata in due schede:

- **Log traffico** - questa scheda fornisce informazioni sull'attività di tutte le applicazioni che hanno tentato di connettersi alla rete. Per ognuna di queste, saranno incluse informazioni relative a ora dell'evento, nome dell'applicazione, rispettiva azione log, nome utente, PID, direzione del traffico, tipo di protocollo, numeri delle porte remote e locali e informazioni sull'indirizzo IP remoto e locale.



- **Log database attendibile** - il *Database attendibile* è un database interno di AVG che raccoglie informazioni sulle applicazioni certificate e attendibili che saranno sempre autorizzate a comunicare online. La prima volta in cui una nuova applicazione tenta di connettersi alla rete (*ossia quando non è ancora stata specificata alcuna regola firewall per tale applicazione*), è necessario stabilire se la comunicazione di rete deve essere consentita per tale applicazione. Innanzitutto, AVG effettua una ricerca nel *Database attendibile*. Se l'applicazione è elencata, sarà automaticamente autorizzata ad accedere alla rete. Se nel database non sono presenti informazioni sull'applicazione, verrà richiesto in una nuova finestra di dialogo se si desidera autorizzare l'applicazione ad accedere alla rete.

#### Pulsanti di controllo

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



### 3.11. Aggiornamenti di AVG

Nessun software di protezione è in grado di garantire una vera protezione dai vari tipi di minacce se non viene aggiornato con regolarità. Gli autori dei virus ricercano di continuo nuove imperfezioni da sfruttare sia nei sistemi operativi che nel software. Tutti i giorni si presentano nuovi virus, nuovi malware e nuovi attacchi di hacker. Per questa ragione, i fornitori di software rilasciano regolarmente aggiornamenti e patch di protezione per correggere eventuali difetti della protezione che vengono rilevati. Considerando le nuove minacce informatiche emergenti e la velocità con cui si diffondono, è assolutamente fondamentale aggiornare **AVG Internet Security** regolarmente. La soluzione migliore è attenersi alle impostazioni predefinite del programma in cui è stato configurato l'aggiornamento automatico. Tenere presente che, se il database dei virus di **AVG Internet Security** non è aggiornato, il programma non sarà in grado di rilevare le minacce più recenti.

***È fondamentale aggiornare AVG con regolarità. Gli aggiornamenti delle definizioni dei virus principali dovrebbero essere eseguiti ogni giorno, se possibile. Gli aggiornamenti del programma meno urgenti possono essere eseguiti settimanalmente.***

Per fornire la protezione massima, **AVG Internet Security** per impostazione predefinita ricerca nuovi aggiornamenti del database dei virus ogni due ore. Poiché gli aggiornamenti AVG non vengono rilasciati in base a una pianificazione fissa, ma in base alla quantità e alla gravità di nuove minacce, questo check-up è molto importante per assicurare che il database dei virus di AVG sia sempre aggiornato.

Per controllare la presenza di nuovi file di aggiornamento immediatamente, utilizzare il collegamento rapido [Aggiorna adesso](#) nell'interfaccia utente principale. Questo collegamento è sempre disponibile da qualsiasi finestra di dialogo dell'[interfaccia utente](#). Una volta avviato l'aggiornamento, AVG verificherà innanzitutto se sono presenti nuovi file di aggiornamento. In caso affermativo, **AVG Internet Security** ne effettuerà il download e avvierà il processo di aggiornamento automaticamente. I risultati dell'aggiornamento verranno visualizzati nella finestra a comparsa sopra l'icona di AVG nell'area di notifica.

Se si desiderasse ridurre il numero di aggiornamenti avviati, è possibile impostare parametri di avvio degli aggiornamenti personalizzati. Tuttavia, **si consiglia di avviare l'aggiornamento almeno una volta al giorno**. La configurazione può essere modificata nella sezione [Impostazioni avanzate/Pianificazioni](#), in particolare nelle seguenti finestre di dialogo:

- [Pianificazione aggiornamento definizioni](#)
- [Pianificazione aggiornamenti Anti-Spam](#)

### 3.12. Domande frequenti e assistenza tecnica

Se si verificano problemi di tipo commerciale o tecnico con l'applicazione **AVG Internet Security**, sono disponibili diversi modi per richiedere assistenza. Effettuare la scelta tra le seguenti opzioni:

- **Ottieni assistenza:** direttamente dall'applicazione AVG è possibile visualizzare una pagina dedicata dell'assistenza clienti sul sito Web di AVG (<http://www.avg.com/>). Selezionare la voce del menu principale **Guida / Ottieni assistenza** per essere reindirizzati a una pagina del sito Web di AVG con le opzioni di assistenza disponibili. Per procedere, seguire le istruzioni fornite nella pagina Web.
- **Assistenza (collegamento nel menu principale):** il menu dell'applicazione AVG (*nella parte superiore dell'interfaccia utente principale*) include il collegamento **Assistenza** che apre una nuova finestra di dialogo contenente tutti i tipi di informazioni necessarie per ricevere assistenza. La finestra di dialogo include dati di base sul programma AVG installato (*versione programma/database*), dettagli della licenza e un elenco di collegamenti rapidi per l'assistenza.





- **Risoluzione dei problemi nella Guida:** una nuova sezione **Risoluzione dei problemi** è disponibile direttamente nel file della Guida incluso in **AVG Internet Security** (per aprire il file della Guida, premere il tasto F1 in qualsiasi finestra di dialogo nell'applicazione). Questa sezione fornisce un elenco delle situazioni che con maggiore frequenza spingono un utente a ricercare assistenza professionale per un problema tecnico. Selezionare la situazione che descrive meglio il problema corrente e fare clic sul collegamento per aprire le istruzioni dettagliate per la risoluzione del problema.
- **Centro di assistenza del sito Web di AVG:** in alternativa, è possibile ricercare la soluzione al problema nel sito Web di AVG (<http://www.avg.com/>). Nella sezione **Assistenza** sono contenuti una panoramica di gruppi tematici che trattano problemi commerciali e tecnici, una sezione strutturata di domande frequenti e tutti i contatti disponibili.
- **AVG ThreatLabs:** un sito Web specifico correlato ad AVG (<http://www.avgthreatlabs.com/website-safety-reports/>) dedicato ai virus, che fornisce una panoramica strutturata delle informazioni relative alle minacce online. Sono inoltre disponibili istruzioni sulla rimozione di virus e spyware e consigli relativi alla protezione.
- **Forum di discussione:** è inoltre possibile utilizzare il forum di discussione degli utenti AVG disponibile all'indirizzo <http://community.avg.com/>.