



AVG Email Server Edition 2011

Manuale per l'utente

Revisione documento 2011.01 (22. 9. 2010)

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

Questo prodotto utilizza l'algoritmo RSA Data Security, Inc. MD5 Message-Digest, Copyright (C) 1991-2, RSA Data Security, Inc. Creazione 1991.

Questo prodotto utilizza il codice dalla libreria C-SaCzech, Copyright (c) 1996-2001 Jaromir Dolecek (dolecek@ics.muni.cz).

Questo prodotto utilizza la libreria di compressione zlib, Copyright (c) 1995-2002 Jean-loup Gailly e Mark Adler



Sommario

1. Introduzione	4
2. Requisiti per l'installazione di AVG	5
2.1 Sistemi operativi supportati	5
2.2 Server e-mail supportati	5
2.3 Requisiti hardware	5
2.4 Disinstalla versioni precedenti	5
2.5 Service Pack di MS Exchange	6
3. Processo di installazione di AVG	7
3.1 Avvio dell'installazione	7
3.2 Attivazione della licenza	8
3.3 Selezionare il tipo di installazione	9
3.4 Installazione personalizzata - Opzioni personalizzate	10
3.5 Completamento dell'installazione	11
4. Scansione e-mail per MS Exchange Server 2007/2010	13
4.1 Panoramica	13
4.2 Scansione e-mail per MS Exchange (routing TA)	16
4.3 Scansione e-mail per MS Exchange (SMTP TA)	18
4.4 Scansione e-mail per MS Exchange (VSAPI)	18
4.5 Avviso tecnico	21
4.6 Azioni di rilevamento	22
4.7 Filtro posta	23
5. Scansione e-mail per MS Exchange Server 2003	24
5.1 Panoramica	24
5.2 Scansione e-mail per MS Exchange (VSAPI)	27
5.3 Azioni di rilevamento	30
5.4 Filtro posta	31
6. AVG per Kerio MailServer	32
6.1 Configurazione	32
6.1.1 Antivirus	32
6.1.2 Filtro allegati	32
7. Configurazione dell'Anti-Spam	37



7.1	Interfaccia dell'Anti-Spam	37
7.2	Principi dell'Anti-Spam	39
7.3	Impostazioni dell'Anti-Spam	39
7.3.1	<i>Procedura guidata apprendimento anti-spam</i>	39
7.3.2	<i>Seleziona cartella con messaggi</i>	39
7.3.3	<i>Opzioni di filtro dei messaggi</i>	39
7.4	Prestazioni	45
7.5	RBL	46
7.6	Whitelist	47
7.7	Blacklist	48
7.8	Impostazioni avanzate	49
8.	AVG Settings Manager	50
9.	Domande frequenti e assistenza tecnica	53



1. Introduzione

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

Complimenti per l'acquisto di AVG Email Server Edition 2011!

AVG Email Server Edition 2011 fa parte della gamma di prodotti pluripremiati AVG progettata per fornire la tranquillità di un'esperienza informatica sicura agli utenti e la protezione completa per il PC. Analogamente a tutti i prodotti AVG, **AVG Email Server Edition 2011** è stato interamente riprogettato per fornire la protezione famosa e accreditata di AVG in una nuova maniera più efficace e intuitiva.

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

Nota: questa documentazione contiene la descrizione di funzionalità specifiche di *E-mail Server Edition*. Se fossero necessarie informazioni su altre funzionalità AVG, consultare il manuale per l'utente di *Internet Security Edition*, che contiene tutti i dettagli necessari. È possibile scaricare il manuale da <http://www.avg.com>.



2. Requisiti per l'installazione di AVG

2.1. Sistemi operativi supportati

AVG Email Server Edition 2011 è destinato alla protezione dei server e-mail che eseguono i seguenti sistemi operativi:

- Windows 2008 Server Edition (x86 e x64)
- Windows 2003 Server (x86, x64) SP1

2.2. Server e-mail supportati

Sono supportati i seguenti server e-mail:

- Versione MS Exchange 2003 Server
- Versione MS Exchange 2007 Server
- Versione MS Exchange 2010 Server
- AVG per Kerio MailServer – versione 6.7.2 e successive

2.3. Requisiti hardware

I requisiti hardware minimi per **AVG Email Server Edition 2011** sono:

- CPU Intel Pentium da 1.5 GHz
- 500 MB di spazio libero sul disco rigido (per l'installazione)
- 512 MB di memoria RAM

I requisiti hardware consigliati per **AVG Email Server Edition 2011** sono:

- CPU Intel Pentium da 1.8 GHz
- 600 MB di spazio libero sul disco rigido (per l'installazione)
- 512 MB di memoria RAM

2.4. Disinstalla versioni precedenti

Se è installata una versione precedente di AVG Email Server, sarà necessario disinstallarla manualmente prima di installare **AVG Email Server Edition 2011**. È necessario eseguire la disinstallazione della versione precedente manualmente, utilizzando la funzionalità standard di Windows.



- Dal menu di avvio **Start/Impostazioni/Pannello di controllo/Installazione applicazioni** selezionare il programma corretto dall'elenco dei software installati. Prestare attenzione a selezionare il programma AVG corretto da disinstallare. È necessario disinstallare Email Server Edition prima di disinstallare AVG File Server Edition.
- Dopo aver disinstallato Email Server Edition, è possibile procedere alla disinstallazione della versione precedente di AVG File Server Edition. Questa operazione può essere eseguita facilmente dal menu di avvio **Start/Tutti i programmi/AVG/Disinstalla AVG**
- Se sono state utilizzate la versione AVG 8.x o versioni precedenti, è necessario disinstallare inoltre i singoli plug-in server.

Nota: sarà necessario riavviare il servizio Archivio informazioni durante il processo di disinstallazione.

Plug-in di Exchange: eseguire setupes.exe con il parametro /uninstall dalla cartella in cui il plug-in è stato installato.

Ad esempio C:\AVG4ES2K\setupes.exe /uninstall

Plug-in di Lotus Domino/Notes: eseguire setupln.exe con il parametro /uninstall dalla cartella in cui il plug-in è stato installato:

Ad esempio C:\AVG4LN\setupln.exe /uninstall

2.5. Service Pack di MS Exchange

Per MS Exchange 2003 Server non è richiesto alcun Service Pack. Tuttavia, si consiglia di mantenere il sistema aggiornato con i Service Pack e gli aggiornamenti rapidi più recenti per ottenere la massima protezione disponibile.

Service Pack per MS Exchange 2003 Server (opzionale):

<http://www.microsoft.com/exchange/evaluation/sp2/overview.msp>

All'inizio dell'installazione verranno esaminate le versioni delle librerie di sistema. Se è necessario installare librerie più recenti, il programma di installazione rinominerà le librerie obsolete con l'estensione .delete. L'eliminazione avverrà dopo il riavvio del sistema.

Service Pack per MS Exchange 2007 Server (opzionale):

<http://www.microsoft.com/downloads/details.aspx?FamilyID=44c66ad6-f185-4a1d-a9ab-473c1188954c&displaylang=en>



3. Processo di installazione di AVG

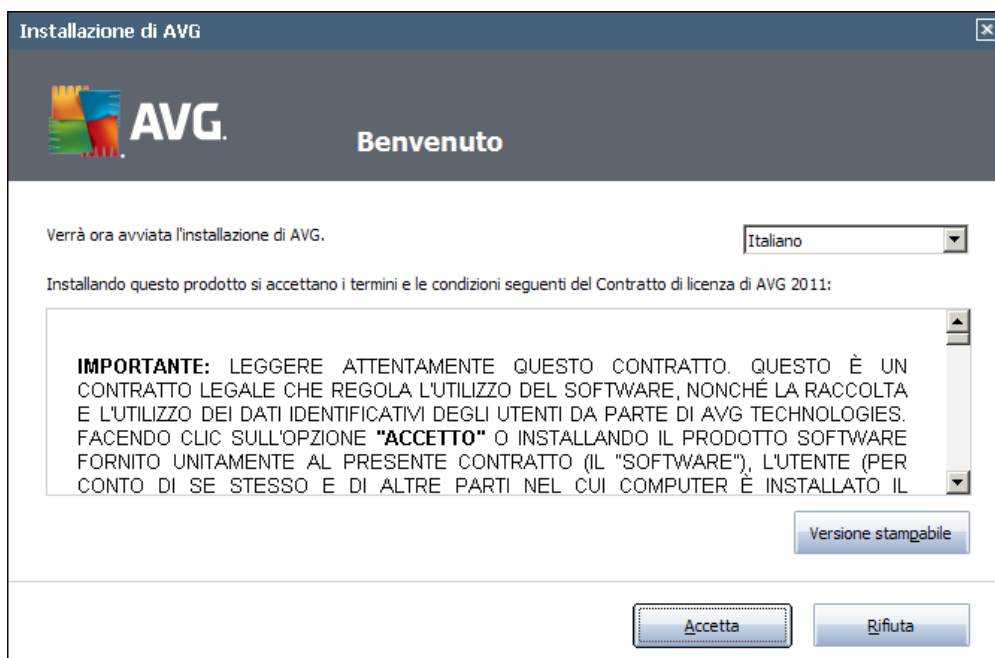
Per installare AVG nel computer è preferibile disporre del file di installazione più recente. È possibile utilizzare il file di installazione presente nel CD contenuto nella confezione del prodotto, tuttavia questo file potrebbe non essere aggiornato. Pertanto è consigliabile procurarsi il file di installazione più recente in linea. È possibile scaricare il file dal [sito Web di AVG](http://www.avg.com/download?prd=msw) (all'indirizzo <http://www.avg.com/download?prd=msw>)

Nota: sono disponibili due pacchetti di installazione per il prodotto, per sistemi operativi a 32 bit (contrassegnato come x86) e per sistemi operativi a 64 bit (contrassegnato come x64). Assicurarsi di utilizzare il pacchetto di installazione corretto per il sistema operativo in uso.

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

Dopo aver scaricato e salvato il file di installazione sul disco rigido, è possibile avviare il processo di installazione. L'installazione consiste in una sequenza di finestre di dialogo contenenti una breve descrizione delle operazioni da eseguire a ogni passaggio. Di seguito viene fornita una descrizione di ciascuna finestra di dialogo:

3.1. Avvio dell'installazione



La prima finestra del processo di installazione visualizzata è quella **introduttiva**. Qui è possibile selezionare la lingua utilizzata per il processo di installazione e leggere le condizioni di licenza. Utilizzare il pulsante **Versione stampabile** per aprire il testo della licenza in una nuova finestra. Selezionare il pulsante **Accetta** per confermare e



procedere alla finestra di dialogo successiva.

Attenzione: sarà inoltre possibile scegliere ulteriori lingue per l'interfaccia dell'applicazione successivamente durante il processo di installazione.

3.2. Attivazione della licenza

Nella finestra di dialogo **Attivazione della licenza** è necessario immettere il numero di licenza.

Immettere il numero di licenza nel campo di testo **Numero di licenza**. Il numero di licenza sarà contenuto nel messaggio e-mail di conferma ricevuto dopo l'acquisto in linea di AVG. È necessario digitare il numero esattamente come viene indicato. Se il numero di licenza è disponibile nel formato digitale (contenuto nel messaggio e-mail), si consiglia di utilizzare il metodo copia/incolla per inserirlo.

Installazione di AVG

AVG. Attivazione della licenza

Numero di licenza:

Esempio: 9FULL-NSDRS-KUL4L-UKSFR-L96M9-B2ALT-XWMX3

Se il software AVG 2011 è stato acquistato in linea, il numero di licenza è stato inviato tramite e-mail. Per evitare errori di battitura, si consiglia di copiare e incollare il numero dall'e-mail in questa schermata.

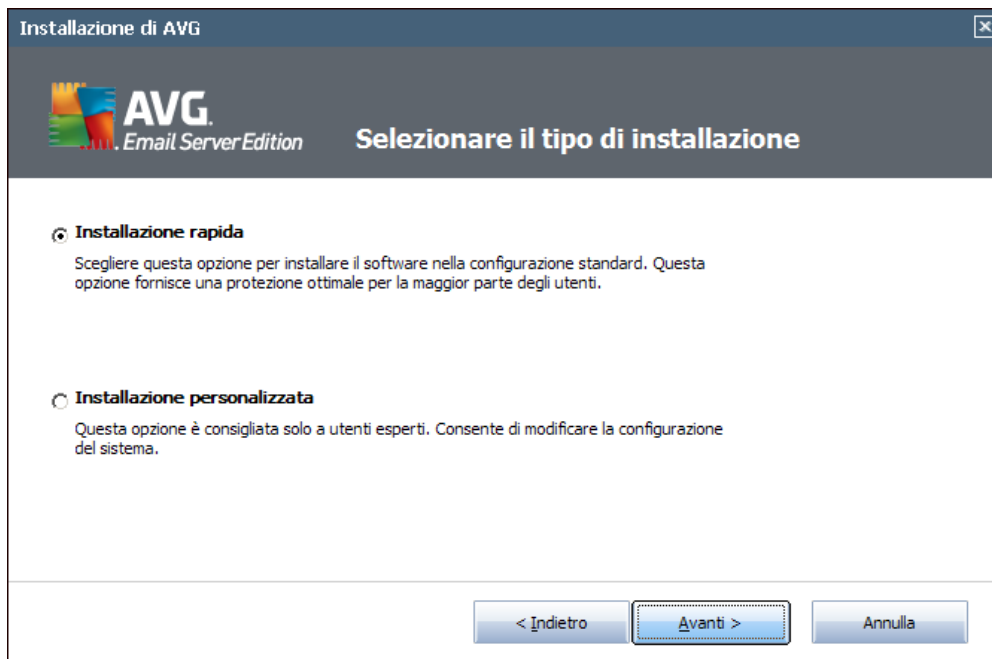
Se il software è stato acquistato in un negozio, il numero di licenza è disponibile nella scheda di registrazione del prodotto inclusa nel pacchetto. Assicurarsi di copiare il numero correttamente.

< Indietro Avanti > Annulla

Selezionare il pulsante **Avanti** per continuare con il processo di installazione.



3.3. Selezionare il tipo di installazione



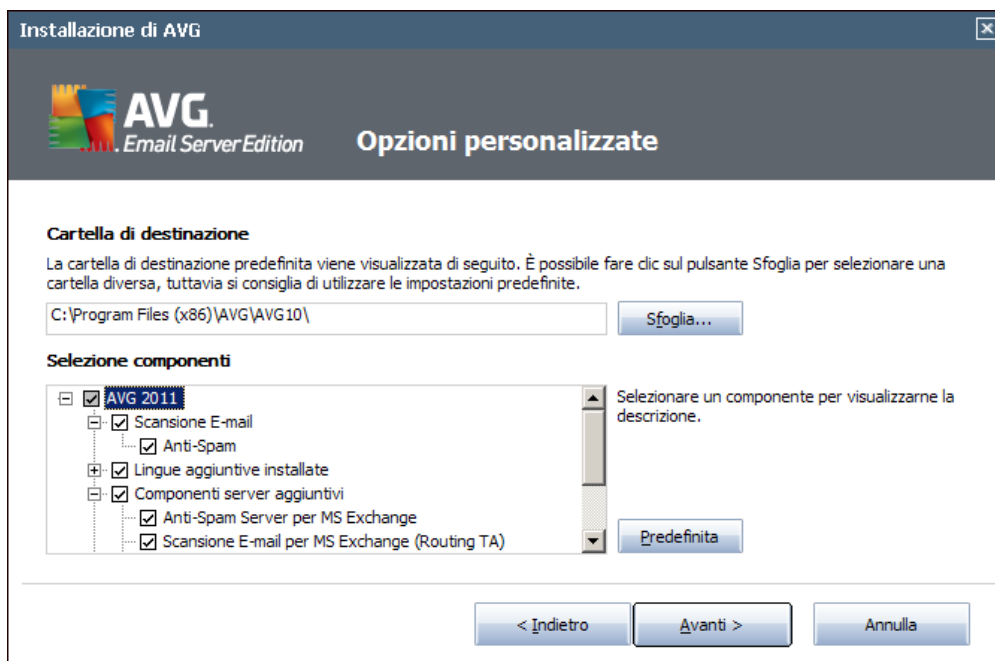
La finestra di dialogo **Selezionare il tipo di installazione** offre due opzioni di installazione: **Installazione rapida** e **Installazione personalizzata**.

Alla maggior parte degli utenti si consiglia di mantenere l'**installazione rapida** che consente di installare AVG in modalità completamente automatica con le impostazioni predefinite dal produttore del software. La configurazione fornisce la massima protezione combinata con l'utilizzo ottimale delle risorse. In futuro, se ci fosse necessità di modificare la configurazione, sarà possibile farlo direttamente nell'applicazione AVG.

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



3.4. Installazione personalizzata - Opzioni personalizzate



La finestra di dialogo **Cartella di destinazione** consente di specificare la posizione di installazione di AVG. Per impostazione predefinita, AVG viene installato nella cartella dei programmi che si trova nell'unità C:. Se si desidera modificare questa posizione, utilizzare il pulsante **Sfoglia** per visualizzare la struttura dell'unità e selezionare la cartella pertinente.

Nella sezione **Selezione componenti** viene visualizzata una panoramica di tutti i componenti di AVG che possono essere installati. Se le impostazioni predefinite non sono adeguate alle esigenze specifiche, è possibile rimuovere/aggiungere determinati componenti.

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

- **AVG Amministrazione remota Client:** se si desidera stabilire la connessione di AVG a AVG DataCenter (AVG Network Edition), è necessario selezionare questa opzione.

Nota: solo i componenti server disponibili nell'elenco possono essere gestiti in remoto.

- **Settings Manager:** strumento adatto soprattutto agli amministratori di rete che consente di copiare, modificare e distribuire la configurazione di AVG. È possibile salvare la configurazione in un dispositivo portatile (unità flash USB e così via), quindi applicarla manualmente o in altro modo alle workstation prescelte.
- **Lingue aggiuntive installate:** è possibile definire in quali lingue installare AVG.



Selezionare la voce **Lingue aggiuntive installate**, quindi scegliere le lingue desiderate dal menu corrispondente.

Panoramica di base dei singoli componenti server (**Componenti server aggiuntivi**):

- **Anti-Spam Server per MS Exchange**

Controlla tutti i messaggi e-mail in entrata e contrassegna i messaggi indesiderati come SPAM. Per elaborare ogni messaggio e-mail vengono utilizzati diversi metodi di analisi che offrono il massimo livello di protezione possibile contro i messaggi e-mail indesiderati.

- **Scansione e-mail per MS Exchange (routing Transport Agent)**

Controlla tutti i messaggi e-mail interni, inviati e ricevuti tramite il ruolo HUB di MS Exchange.

Disponibile per MS Exchange 2007/2010, può essere installato esclusivamente per il ruolo HUB.

- **Scansione e-mail per MS Exchange (SMTP Transport Agent).**

Controlla tutti i messaggi e-mail ricevuti tramite l'interfaccia MS Exchange SMTP.

Disponibile esclusivamente per MS Exchange 2007/2010, può essere installato per ruoli EDGE e HUB.

- **Scansione e-mail per MS Exchange (VSAPI)**

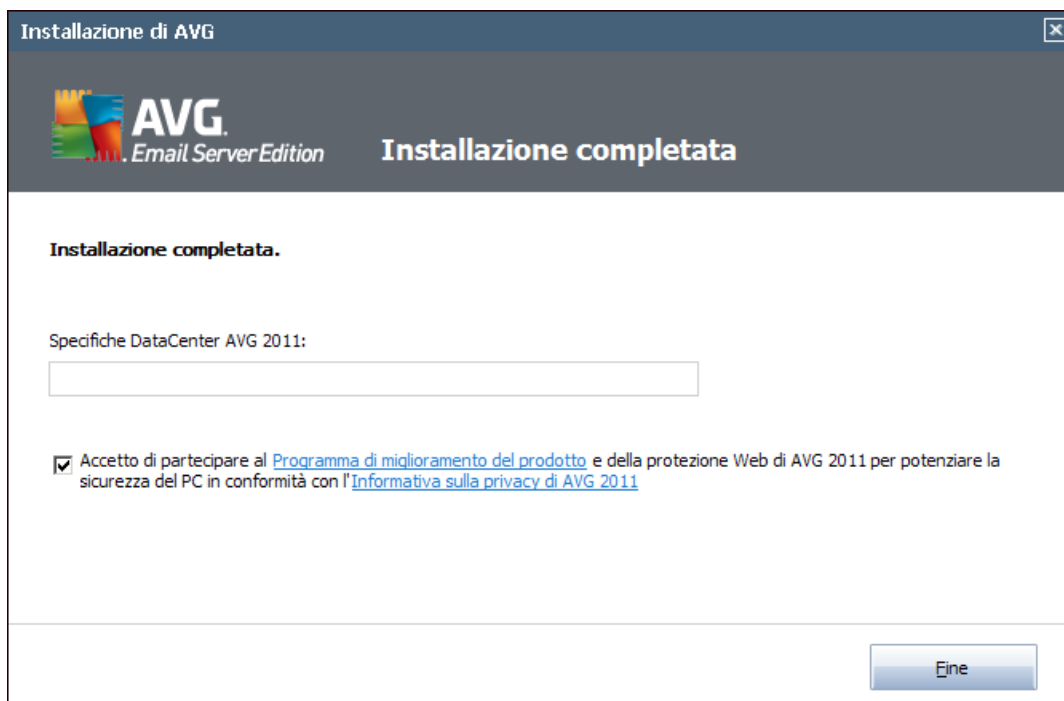
Controlla tutti i messaggi e-mail archiviati nelle cassette postali degli utenti. Se vengono rilevati virus, questi vengono spostati in quarantena o completamente rimossi.

Nota: sono disponibili diverse opzioni per diverse versioni di MS Exchange.

Continuare selezionando il pulsante **Avanti**.

3.5. Completamento dell'installazione

Se è stato selezionato il modulo **Componente Amministrazione remota** durante la selezione dei moduli, la schermata finale consente di definire la stringa di connessione a AVG DataCenter.



AVG è ora installato nel computer e funziona correttamente. Il programma viene eseguito in background in modalità completamente automatica.

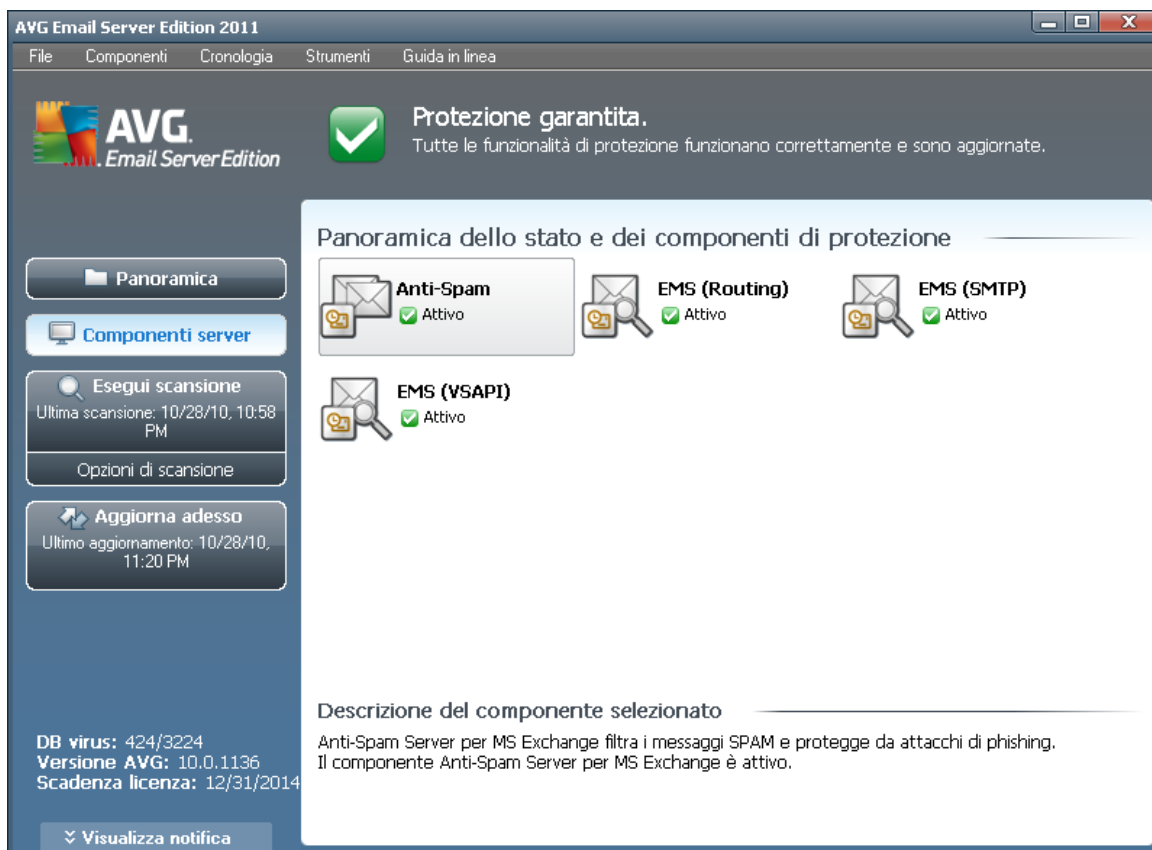
Per configurare la protezione individualmente per il server e-mail, consultare il capitolo appropriato:

- [**Scansione e-mail per MS Exchange Server 2007/2010**](#)
- [**Scansione e-mail per MS Exchange Server 2003**](#)
- [**AVG per Kerio MailServer**](#)

4. Scansione e-mail per MS Exchange Server 2007/2010

4.1. Panoramica

Le opzioni di configurazione di AVG per MS Exchange Server 2007/2010 sono completamente integrate in AVG Email Server Edition 2011 come componenti server.



The screenshot displays the AVG Email Server Edition 2011 management console. At the top, a green checkmark icon indicates 'Protezione garantita.' (Protection guaranteed) with the note 'Tutte le funzionalità di protezione funzionano correttamente e sono aggiornate.' (All protection features are working correctly and are updated). Below this, a section titled 'Panoramica dello stato e dei componenti di protezione' (Overview of the status and protection components) shows four components, all marked as 'Attivo' (Active): Anti-Spam, EMS (Routing), EMS (SMTP), and EMS (VSAPI). On the left sidebar, there are buttons for 'Panoramica', 'Componenti server', 'Esegui scansione' (with the last scan on 10/28/10 at 10:58 PM), 'Opzioni di scansione', and 'Aggiorna adesso' (with the last update on 10/28/10 at 11:20 PM). At the bottom left, system information is provided: 'DB virus: 424/3224', 'Versione AVG: 10.0.1136', and 'Scadenza licenza: 12/31/2014'. A 'Visualizza notifica' button is located at the bottom left of the main content area.

Panoramica di base dei singoli componenti server:

- **[Anti-Spam - Anti-Spam Server per MS Exchange](#)**

Controlla tutti i messaggi e-mail in entrata e contrassegna i messaggi indesiderati come SPAM. Per elaborare ogni messaggio e-mail vengono utilizzati diversi metodi di analisi che offrono il massimo livello di protezione possibile contro i messaggi e-mail indesiderati.

- **[EMS \(routing\) - Scansione e-mail per MS Exchange \(routing Transport Agent\)](#)**

Controlla tutti i messaggi e-mail interni, inviati e ricevuti tramite il ruolo HUB di MS Exchange.



Disponibile per MS Exchange 2007/2010, può essere installato esclusivamente per il ruolo HUB.

- **[EMS \(SMTP\) - Scansione e-mail per MS Exchange \(SMTP Transport Agent\)](#)**

Controlla tutti i messaggi e-mail ricevuti tramite l'interfaccia MS Exchange SMTP.

Disponibile esclusivamente per MS Exchange 2007/2010, può essere installato per ruoli EDGE e HUB.

- **[EMS \(VSAPI\) - Scansione e-mail per MS Exchange \(VSAPI\)](#)**

Controlla tutti i messaggi e-mail archiviati nelle cassette postali degli utenti. Se vengono rilevati virus, questi vengono spostati in quarantena o completamente rimossi.

Nota importante: se si è scelto di installare e utilizzare VSAPI in combinazione con il Routing Transport Agent su un ruolo Exchange Hub, i messaggi e-mail verranno sottoposti a scansione due volte. Per evitarlo, consultare il capitolo [Avviso tecnico](#) di seguito per ulteriori dettagli.

Fare doppio clic sul componente desiderato per aprirne l'interfaccia. Con l'eccezione di Anti-Spam, tutti i componenti condividono i seguenti pulsanti di controllo e collegamenti comuni:

The screenshot displays the AVG Email Server Edition 2011 interface. At the top, there is a menu bar with 'File', 'Componenti', 'Cronologia', 'Strumenti', and 'Guida in linea'. Below the menu, the AVG logo and 'Email Server Edition' are visible. A green checkmark icon indicates 'Protezione garantita. Tutte le funzionalità di protezione funzionano correttamente e sono aggiornate.'

The main content area is titled 'Componente Scansione E-mail per MS Exchange (Routing TA)'. It features a description: 'Scansione E-mail per MS Exchange (Routing TA) controlla tutti i messaggi e-mail distribuiti tramite il ruolo server HUB di MS Exchange. Se rilevati, i virus vengono spostati in Quarantena virus o completamente rimossi.'

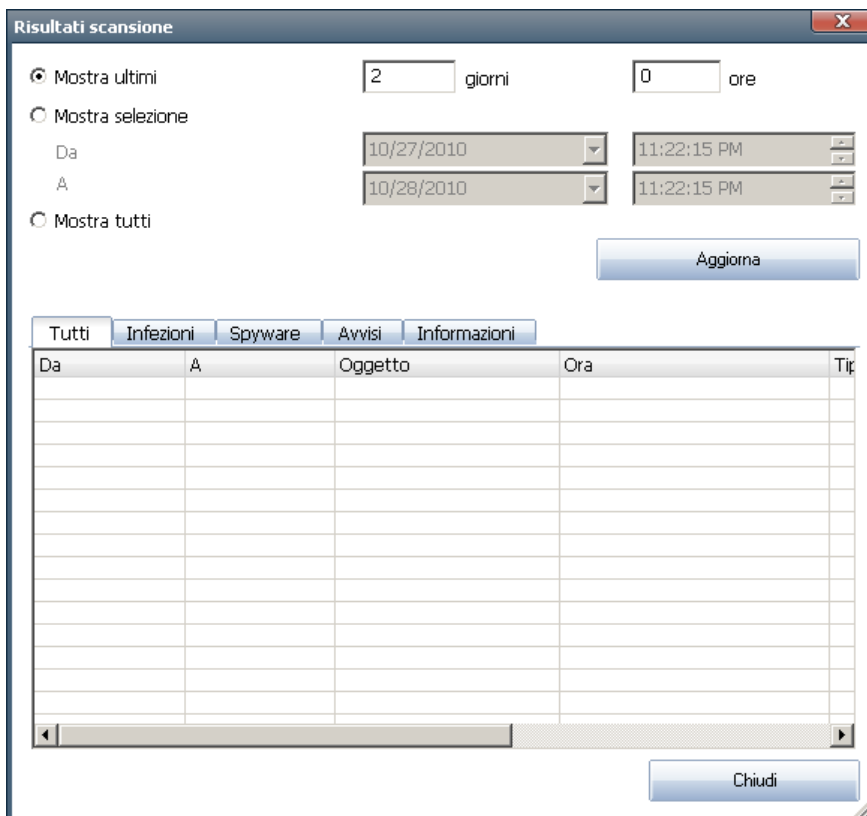
Below the description, there is a green checkmark icon and the text 'Attivo'. A summary table shows: 'Messaggi e-mail controllati: 0 da 10/20/2010, 12:08 AM' and 'Minacce rilevate: 0 da 10/20/2010, 12:08 AM'. There are links for 'Risultati scansione', 'Aggiorna valori statistici', and 'Ripristina i valori statistici'.

On the left side, there is a sidebar with several buttons: 'Panoramica', 'Componenti server' (with a sub-button for 'Scansione E-mail per MS Exchange (Routing TA)'), 'Esegui scansione' (with 'Ultima scansione: 10/28/10, 10:58 PM' and 'Opzioni di scansione'), and 'Aggiorna adesso' (with 'Ultimo aggiornamento: 10/28/10, 11:20 PM').

At the bottom left, there is a 'Visualizza notifica' button. At the bottom right, there are 'Impostazioni' and 'Indietro' buttons. The bottom status bar shows: 'DB virus: 424/3224', 'Versione AVG: 10.0.1136', and 'Scadenza licenza: 12/31/2014'.

- **Risultati scansione**

Aprire una nuova finestra di dialogo in cui è possibile visualizzare i risultati della scansione:



Qui è possibile visualizzare i messaggi divisi in diverse schede in base alla relativa gravità. Vedere la configurazione dei singoli componenti per modificare gravità e segnalazione.

Per impostazione predefinita, vengono visualizzati solo i risultati relativi agli ultimi due giorni. È possibile cambiare il periodo visualizzato modificando le seguenti opzioni:

- **Mostra ultimi:** immettere i giorni e le ore prescelti.
- **Mostra selezione:** scegliere un intervallo di ora e data personalizzato.
- **Mostra tutti:** visualizza i risultati relativi all'intero periodo.

Utilizzare il pulsante **Aggiorna** per ricaricare i risultati.

- **Aggiorna valori statistici:** aggiorna le statistiche visualizzate in alto.
- **Reimposta valori statistici:** reimposta tutte le statistiche su zero.

I pulsanti attivi sono:

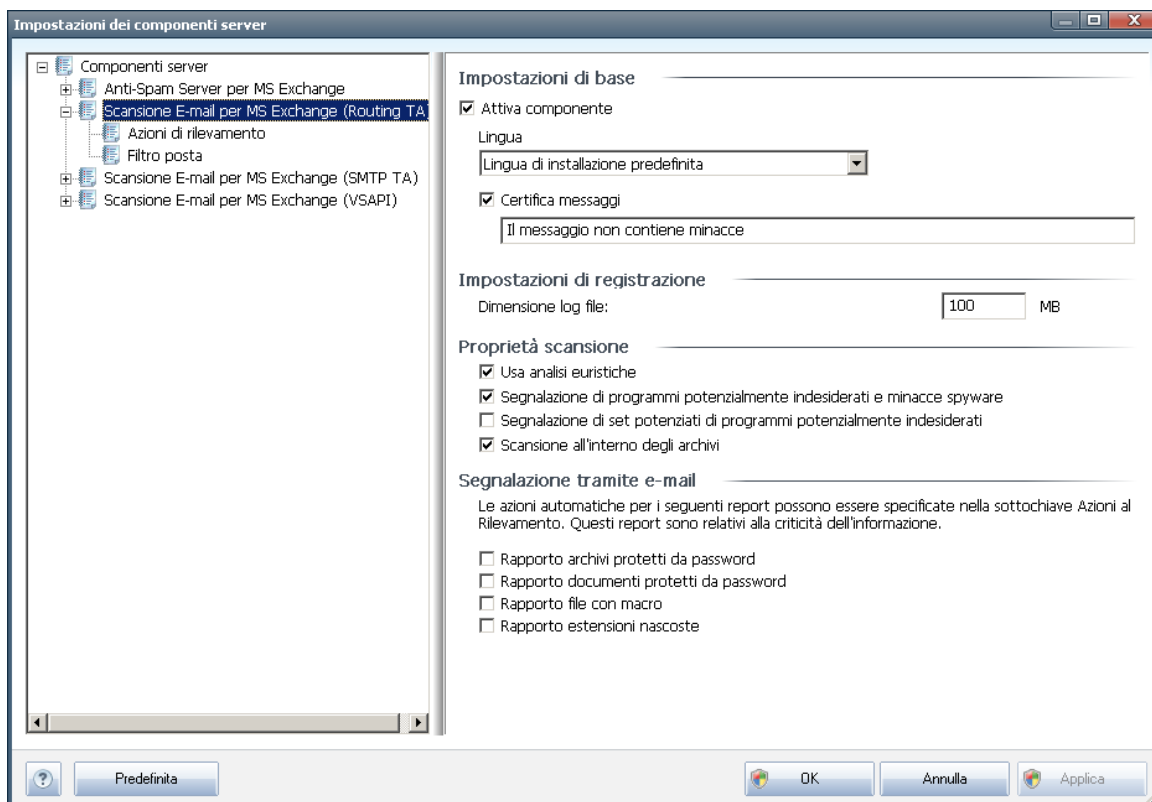
- **Impostazioni:** utilizzare questo pulsante per aprire le impostazioni del componente.
- **Indietro:** selezionare questo pulsante per tornare alla panoramica dei componenti server.

Nei seguenti capitoli sono disponibili ulteriori informazioni sulle singole impostazioni di tutti i componenti.

4.2. Scansione e-mail per MS Exchange (routing TA)

Per aprire le impostazioni di **Scansione e-mail per MS Exchange (routing TA)**, selezionare il pulsante **Impostazioni** dall'interfaccia del componente.

Dall'elenco **Componenti server** selezionare la voce **Scansione e-mail per MS Exchange (routing TA)**:



La sezione **Impostazioni di base** contiene le seguenti opzioni:

- **Attiva componente:** deselezionare l'opzione per disattivare l'intero componente.
- **Lingua:** selezionare la lingua del componente desiderata.



- **Certifica messaggi:** selezionare questa opzione per aggiungere una nota di certificazione a tutti i messaggi sottoposti a scansione. È possibile personalizzare il messaggio nel campo successivo.

La sezione **Impostazioni di registrazione:**

- **Dimensione log file:** selezionare le dimensioni desiderate del file log. Valore predefinito: 100 MB.

La sezione **Proprietà scansione:**

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

La sezione **Segnalazione allegati e-mail** consente di scegliere quali elementi devono essere segnalati durante la scansione. Se questa opzione è selezionata, ciascuna e-mail che include un elemento simile conterrà il tag [INFORMATION] nell'oggetto del messaggio. Questa è la configurazione predefinita che può essere facilmente modificata nella sezione **Azioni di rilevamento, Informazioni** (vedere di seguito).

Sono disponibili le seguenti opzioni:

- **Segnala archivi protetti da password**
- **Segnala documenti protetti da password**
- **Segnala file contenenti macro**
- **Segnala estensioni nascoste**

Sono inoltre disponibili le presenti sottovoci nella seguente struttura:



- [Azioni di rilevamento](#)
- [Filtro posta](#)

4.3. Scansione e-mail per MS Exchange (SMTP TA)

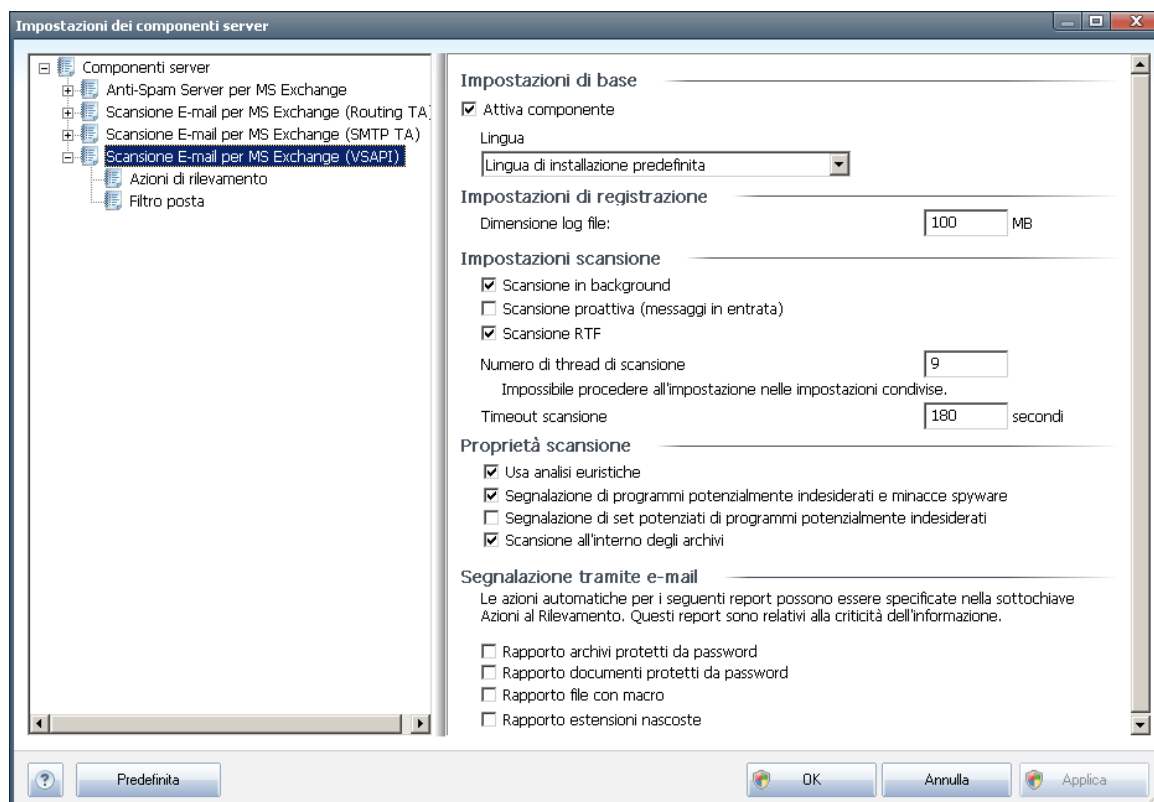
La configurazione di **Scansione e-mail per MS Exchange (SMTP Transport Agent)** è esattamente uguale in caso di routing transport agent. Per ulteriori informazioni consultare il capitolo precedente [Scansione e-mail per MS Exchange \(routing TA\)](#).

Sono inoltre disponibili le presenti sottovoci nella seguente struttura:

- [Azioni di rilevamento](#)
- [Filtro posta](#)

4.4. Scansione e-mail per MS Exchange (VSAPI)

Questa voce contiene le impostazioni di **Scansione e-mail per MS Exchange (VSAPI)**.



La sezione **Impostazioni di base** contiene le seguenti opzioni:

- **Attiva componente:** deselezionare l'opzione per disattivare l'intero componente.



- **Lingua:** selezionare la lingua del componente desiderata.

La sezione **Impostazioni di registrazione:**

- **Dimensione log file:** selezionare le dimensioni desiderate del file log. Valore predefinito: 100 MB.

La sezione **Impostazioni scansione:**

- **Scansione in background:** consente di abilitare o disabilitare il processo di scansione in background. La scansione in background è una delle funzionalità dell'interfaccia applicativa VSAPI 2.0/2.5. Fornisce la scansione in base ai thread dei database di messaggistica di Exchange. Se all'interno delle cartelle della casella di posta dell'utente viene rilevato un elemento che non è stato sottoposto a scansione con l'aggiornamento più recente del database dei virus, tale elemento viene inviato a AVG per Exchange Server per essere sottoposto a scansione. La scansione e la ricerca di oggetti non esaminati vengono eseguite in parallelo.

Un thread specifico a bassa priorità viene utilizzato per ciascun database e ciò garantisce che altre attività (ad esempio l'archiviazione di messaggi e-mail nel database Microsoft Exchange) vengano sempre eseguite come preferenziali.

- **Scansione proattiva (messaggi in arrivo)**

È possibile abilitare o disabilitare la scansione proattiva di VSAPI 2.0/2.5 qui. Questo tipo di scansione viene effettuato quando un elemento viene spostato in una cartella senza che sia stata effettuata alcuna richiesta da parte del client.

Non appena i messaggi vengono inviati all'archivio Exchange, vengono aggiunti alla coda di scansione globale a bassa priorità (massimo 30 elementi). Questi vengono sottoposti a scansione in base al metodo FIFO (primo entrato, primo uscito). Se si accede a un elemento che si trova in tale coda, esso assume elevata priorità.

Nota: i messaggi di overflow continueranno a essere memorizzati senza essere sottoposti a scansione.

Nota: anche se si disattivano entrambe le opzioni **Scansione in background** e **Scansione proattiva**, la scansione all'accesso sarà comunque attiva quando l'utente tenterà di scaricare un messaggio con il client MS Outlook.

- **Scansione RTF:** consente di specificare se eseguire la scansione del tipo di file RTF.
- **Numero di thread di scansione:** per impostazione predefinita, il processo di scansione viene suddiviso in thread per migliorare le prestazioni globali della scansione grazie a un determinato livello di parallelismo. Qui è possibile modificare il numero dei thread.

Il numero predefinito di thread è calcolato come 2 volte il "numero dei processori" + 1.



Il numero minimo di thread è calcolato come ("numero dei processori" +1) diviso 2.

Il numero massimo di thread è calcolato come "numero dei processori" moltiplicato per 5 + 1.

Se il valore corrisponde o è inferiore al minimo oppure corrisponde o è superiore al massimo, verrà utilizzato il valore predefinito.

- **Timeout scansione:** l'intervallo massimo continuo (in secondi) di accesso al messaggio in fase di scansione da parte di un thread (il valore predefinito è 180 secondi).

La sezione **Proprietà scansione:**

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

La sezione **Segnalazione allegati e-mail** consente di scegliere quali elementi devono essere segnalati durante la scansione. La configurazione predefinita può essere modificata facilmente nella sezione **Azioni di rilevamento, Informazioni** (vedere sotto).

Sono disponibili le seguenti opzioni:

- **Segnala archivi protetti da password**
- **Segnala documenti protetti da password**
- **Segnala file contenenti macro**
- **Segnala estensioni nascoste**



In genere, alcune di queste funzioni sono estensioni per l'utente dei servizi dell'interfaccia applicativa Microsoft VSAPI 2.0/2.5. Per informazioni dettagliate su VSAPI 2.0/2.5, vedere i seguenti collegamenti e i collegamenti accessibili tramite essi:

- <http://support.microsoft.com/default.aspx?scid=kb;en-us;328841&Product=exch2k> per informazioni sull'interazione tra il software antivirus e Exchange
- <http://support.microsoft.com/default.aspx?scid=kb;en-us;823166> per informazioni sulle funzionalità aggiuntive di VSAPI 2.5 in Exchange 2003 Server.

Sono inoltre disponibili le presenti sottovoci nella seguente struttura:

- [**Azioni di rilevamento**](#)
- [**Filtro posta**](#)

4.5. Avviso tecnico

Queste informazioni si riferiscono a una situazione in cui siano installati e in uso VSAPI e Routing Transport Agent su un ruolo Exchange Hub. In tal caso, i messaggi e-mail verranno sottoposti a scansione due volte (prima dalla scansione all'accesso VSAPI, quindi dal Routing Transport Agent).

A causa del funzionamento tipico dell'interfaccia VSAPI, potrebbero verificarsi incoerenze nei risultati di scansione nonché carichi non necessari. Pertanto, per evitare la doppia scansione, si consiglia di utilizzare una soluzione di correzione (vedere di seguito) in grado di risolvere il problema immediatamente.

Nota: *la regolazione del registro è consigliata solo a utenti esperti. Prima di modificare il registro, effettuarne il backup e prevedere come ripristinarlo in caso di problemi.*

Aprire l'editor di registro (menu di Windows **Start/Esegui**, digitare **regedit** e premere Invio). Accedere al seguente ramo:

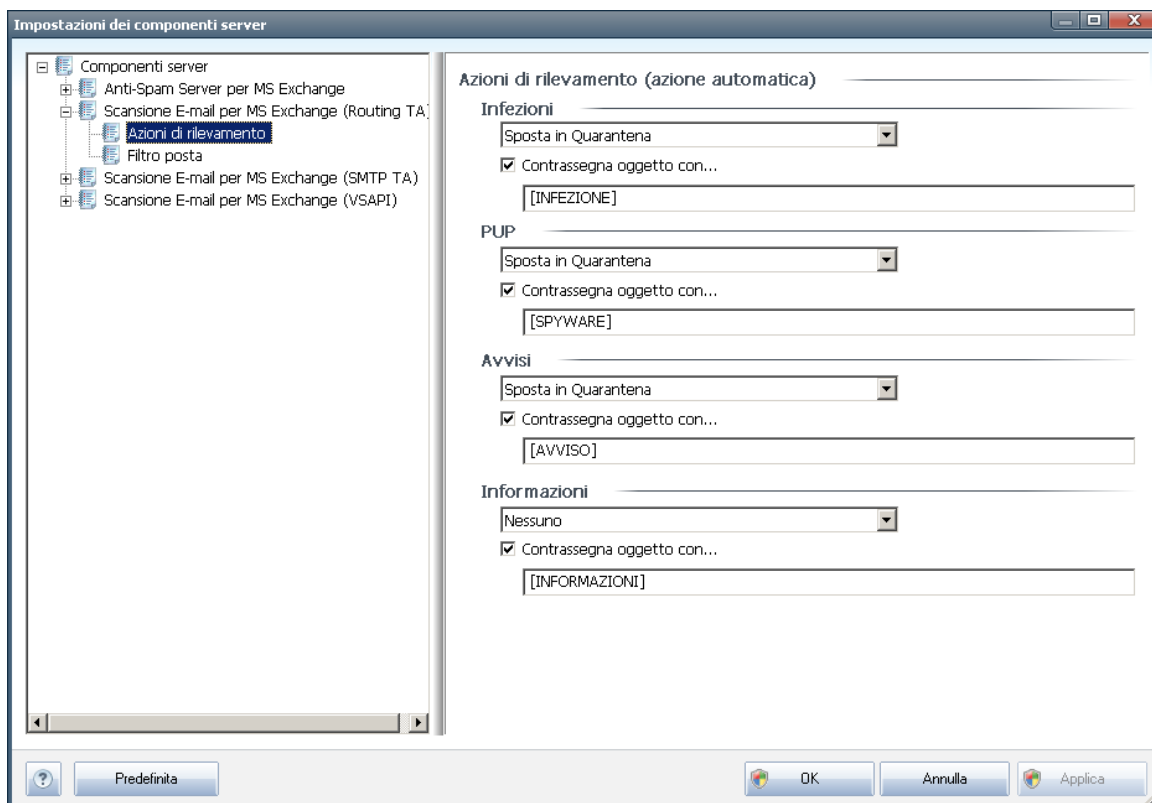
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeIS\ViruScan

Fare clic con il pulsante destro del mouse nella parte destra della finestra e dal menu di scelta rapida selezionare **Nuovo/Valore DWORD (32 bit)**. Denominare il nuovo valore **TransportExclusion**. Una volta creato, fare doppio clic su di esso e modificarne il valore in **1**.

Infine, per applicare le modifiche al server MS Exchange, è necessario impostare il valore di **ReloadNow** su 1. Per farlo, fare doppio clic su di esso e modificarne il valore.

In questo modo vengono disattivate le scansioni in uscita dalla scansione all'accesso VSAPI. La modifica dovrebbe risultare attiva dopo pochi minuti.

4.6. Azioni di rilevamento



Nella sottovoce **Azioni di rilevamento** è possibile selezionare le azioni automatiche da eseguire durante il processo di scansione.

Tali azioni sono disponibili per le seguenti voci:

- **Infezioni**
- **Programmi potenzialmente indesiderati (PUP, Potentially Unwanted Programs)**
- **Avvisi**
- **Informazioni**

Utilizzare il menu a discesa per selezionare un'azione per ciascuna voce:

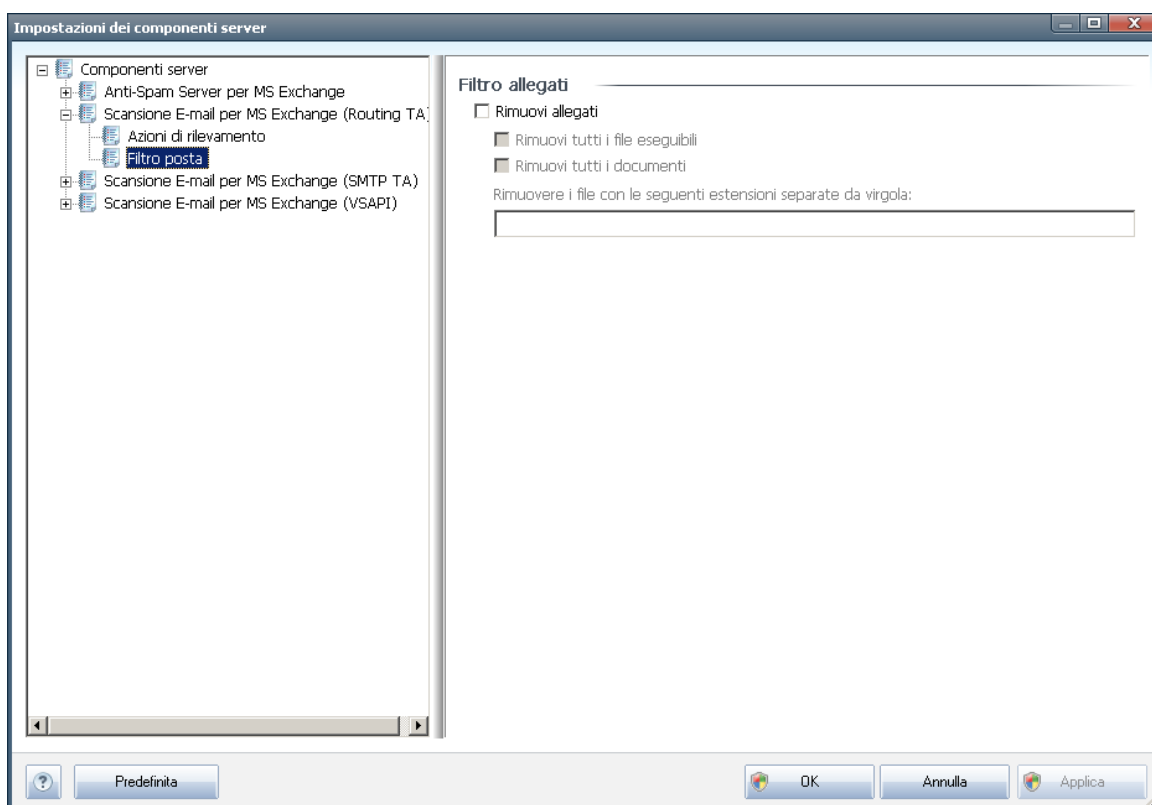
- **Nessuna** - non verrà eseguita nessuna azione.
- **Sposta in Quarantena** - la minaccia verrà spostata in Quarantena virus.
- **Rimuovi** - la minaccia verrà rimossa.

Per selezionare un oggetto personalizzato per i messaggi che contengono un

determinato elemento/minaccia, selezionare la casella **Contrassegna oggetto con...** ed immettere il valore preferito.

Nota: l'ultima funzione citata non è disponibile per Scansione e-mail per MS Exchange VSAPI.

4.7. Filtro posta



Nella sottovoce **Filtro posta** è possibile selezionare gli eventuali allegati da rimuovere automaticamente. Sono disponibili le seguenti opzioni:

- **Rimuovi allegati** - selezionare questa casella per abilitare la funzione.
- **Rimuovi tutti i file eseguibili** - consente di rimuovere tutti i file eseguibili.
- **Rimuovi tutti i documenti** - consente di rimuovere tutti i documenti.
- **Rimuovere i file con le seguenti estensioni separate da virgola** - selezionare le caselle con le estensioni che si desidera rimuovere automaticamente. Separare le estensioni con una virgola.



5. Scansione e-mail per MS Exchange Server 2003

5.1. Panoramica

Le opzioni di configurazione di Scansione e-mail per MS Exchange Server 2003 sono completamente integrate in AVG Email Server Edition 2011 come componenti server.



I componenti server includono:

Panoramica di base dei singoli componenti server:

- **[Anti-Spam - Anti-Spam Server per MS Exchange](#)**

Controlla tutti i messaggi e-mail in entrata e contrassegna i messaggi indesiderati come SPAM. Per elaborare ogni messaggio e-mail vengono utilizzati diversi metodi di analisi che offrono il massimo livello di protezione possibile contro i messaggi e-mail indesiderati.

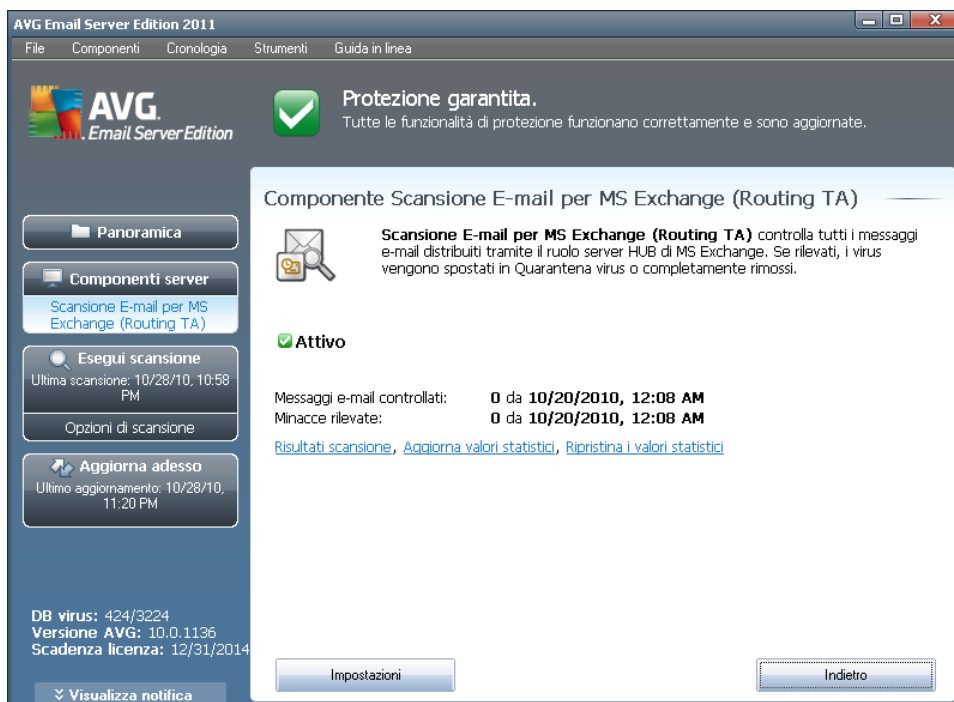
- **[EMS \(VSAPI\) - Scansione e-mail per MS Exchange \(VSAPI\)](#)**

Controlla tutti i messaggi e-mail archiviati nelle cassette postali degli utenti. Se vengono rilevati virus, questi vengono spostati in quarantena o completamente



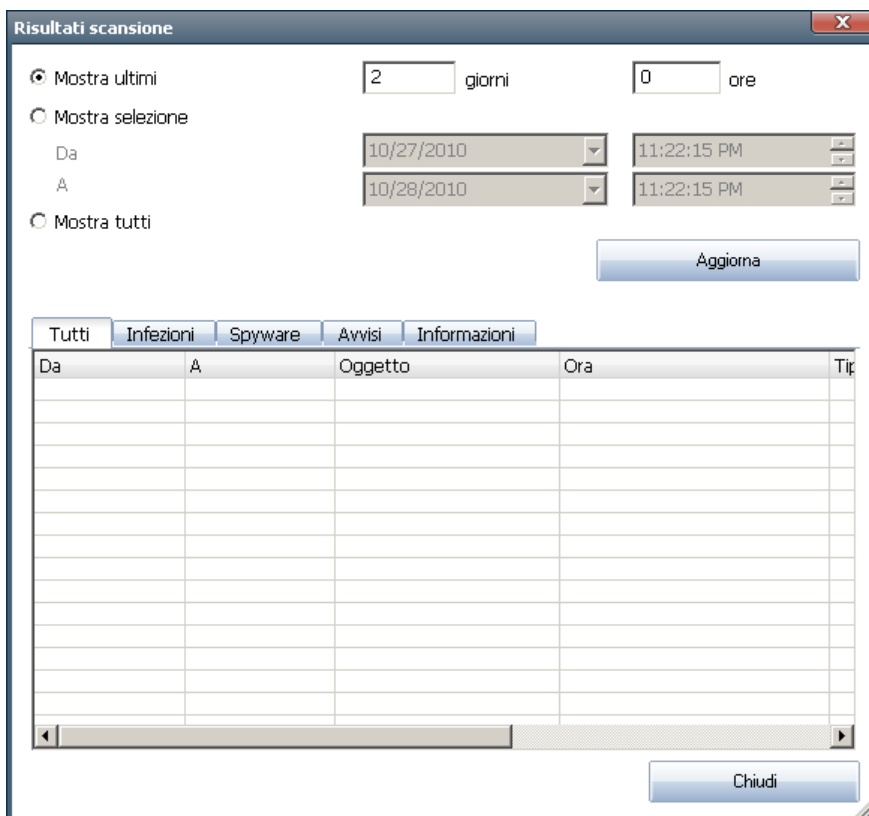
rimossi.

Fare doppio clic sul componente desiderato per aprirne l'interfaccia. Con l'eccezione di Anti-Spam, tutti i componenti condividono i seguenti pulsanti di controllo e collegamenti comuni:



- **Risultati scansione**

Aprire una nuova finestra di dialogo in cui è possibile visualizzare i risultati della scansione:



Qui è possibile visualizzare i messaggi divisi in diverse schede in base alla relativa gravità. Vedere la configurazione dei singoli componenti per modificare gravità e segnalazione.

Per impostazione predefinita, vengono visualizzati solo i risultati relativi agli ultimi due giorni. È possibile cambiare il periodo visualizzato modificando le seguenti opzioni:

- **Mostra ultimi:** immettere i giorni e le ore prescelti.
- **Mostra selezione:** scegliere un intervallo di ora e data personalizzato.
- **Mostra tutti:** visualizza i risultati relativi all'intero periodo.

Utilizzare il pulsante **Aggiorna** per ricaricare i risultati.

- **Aggiorna valori statistici:** aggiorna le statistiche visualizzate in alto.
- **Reimposta valori statistici:** reimposta tutte le statistiche su zero.

I pulsanti attivi sono:

- **Impostazioni:** utilizzare questo pulsante per aprire le impostazioni del componente.

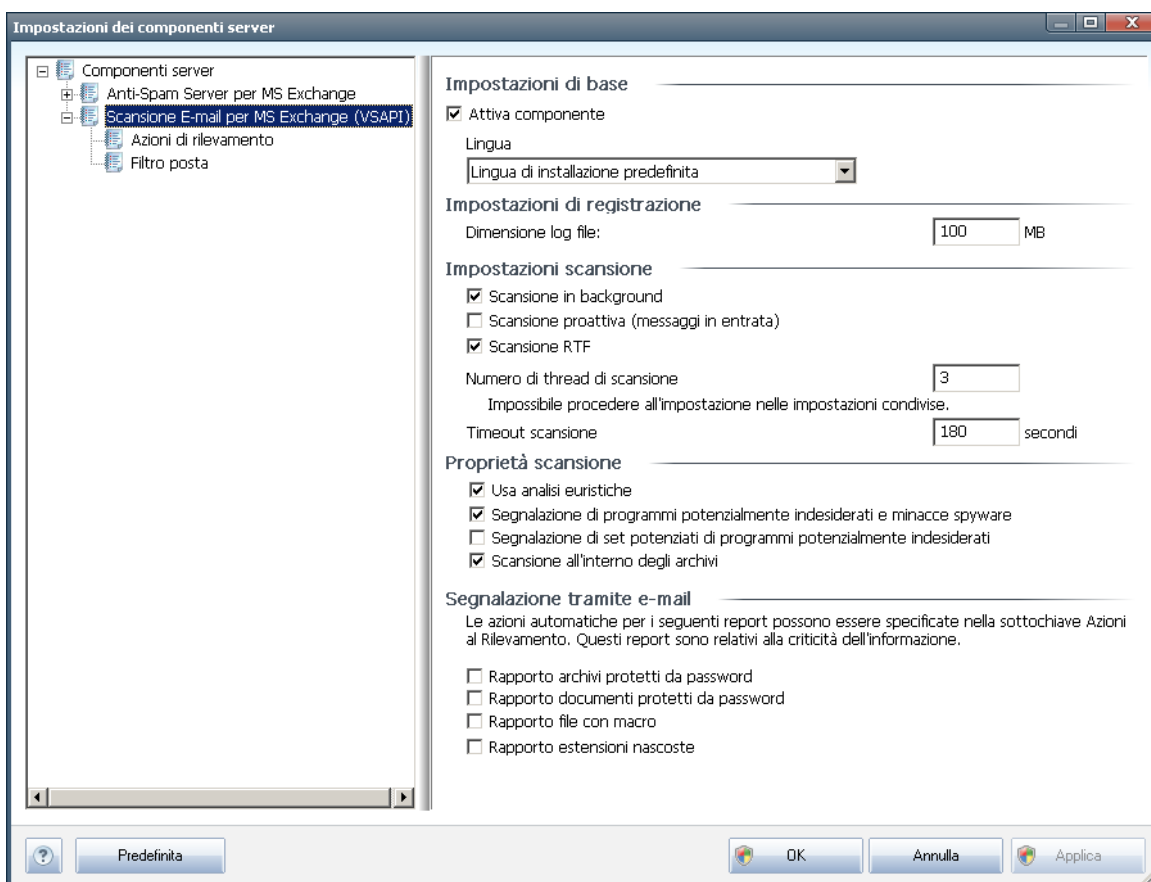


- **Indietro**: selezionare questo pulsante per tornare alla panoramica dei componenti server.

Nei seguenti capitoli sono disponibili ulteriori informazioni sulle singole impostazioni di tutti i componenti.

5.2. Scansione e-mail per MS Exchange (VSAPI)

Questa voce contiene le impostazioni di **Scansione e-mail per MS Exchange (VSAPI)**.



La sezione **Impostazioni di base** contiene le seguenti opzioni:

- **Attiva componente**: deselezionare l'opzione per disattivare l'intero componente.
- **Lingua**: selezionare la lingua del componente desiderata.

La sezione **Impostazioni di registrazione**:

- **Dimensione log file**: selezionare le dimensioni desiderate del file log. Valore predefinito: 100 MB.

La sezione **Impostazioni scansione**:



- **Scansione in background:** consente di abilitare o disabilitare il processo di scansione in background. La scansione in background è una delle funzionalità dell'interfaccia applicativa VSAPI 2.0/2.5. Fornisce la scansione in base ai thread dei database di messaggistica di Exchange. Se all'interno delle cartelle della casella di posta dell'utente viene rilevato un elemento che non è stato sottoposto a scansione con l'aggiornamento più recente del database dei virus, tale elemento viene inviato a AVG per Exchange Server per essere sottoposto a scansione. La scansione e la ricerca di oggetti non esaminati vengono eseguite in parallelo.

Un thread specifico a bassa priorità viene utilizzato per ciascun database e ciò garantisce che altre attività (ad esempio l'archiviazione di messaggi e-mail nel database Microsoft Exchange) vengano sempre eseguite come preferenziali.

- **Scansione proattiva (messaggi in arrivo)**

È possibile abilitare o disabilitare la scansione proattiva di VSAPI 2.0/2.5 qui. Questo tipo di scansione viene effettuato quando un elemento viene spostato in una cartella senza che sia stata effettuata alcuna richiesta da parte del client.

Non appena i messaggi vengono inviati all'archivio Exchange, vengono aggiunti alla coda di scansione globale a bassa priorità (massimo 30 elementi). Questi vengono sottoposti a scansione in base al metodo FIFO (primo entrato, primo uscito). Se si accede a un elemento che si trova in tale coda, esso assume elevata priorità.

Nota: i messaggi di overflow continueranno a essere memorizzati senza essere sottoposti a scansione.

Nota: anche se si disattivano entrambe le opzioni **Scansione in background** e **Scansione proattiva**, la scansione all'accesso sarà comunque attiva quando l'utente tenterà di scaricare un messaggio con il client MS Outlook.

- **Scansione RTF:** consente di specificare se eseguire la scansione del tipo di file RTF.
- **Numero di thread di scansione:** per impostazione predefinita, il processo di scansione viene suddiviso in thread per migliorare le prestazioni globali della scansione grazie a un determinato livello di parallelismo. Qui è possibile modificare il numero dei thread.

Il numero predefinito di thread è calcolato come 2 volte il "numero dei processori" + 1.

Il numero minimo di thread è calcolato come ("numero dei processori" +1) diviso 2.

Il numero massimo di thread è calcolato come "numero dei processori" moltiplicato per 5 + 1.

Se il valore corrisponde o è inferiore al minimo oppure corrisponde o è superiore al massimo, verrà utilizzato il valore predefinito.



- **Timeout scansione:** l'intervallo massimo continuo (in secondi) di accesso al messaggio in fase di scansione da parte di un thread (il valore predefinito è 180 secondi).

La sezione **Proprietà scansione:**

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

La sezione **Segnalazione allegati e-mail** consente di scegliere quali elementi devono essere segnalati durante la scansione. La configurazione predefinita può essere modificata facilmente nella sezione **Azioni di rilevamento, Informazioni** (vedere sotto).

Sono disponibili le seguenti opzioni:

- **Segnala archivi protetti da password**
- **Segnala documenti protetti da password**
- **Segnala file contenenti macro**
- **Segnala estensioni nascoste**

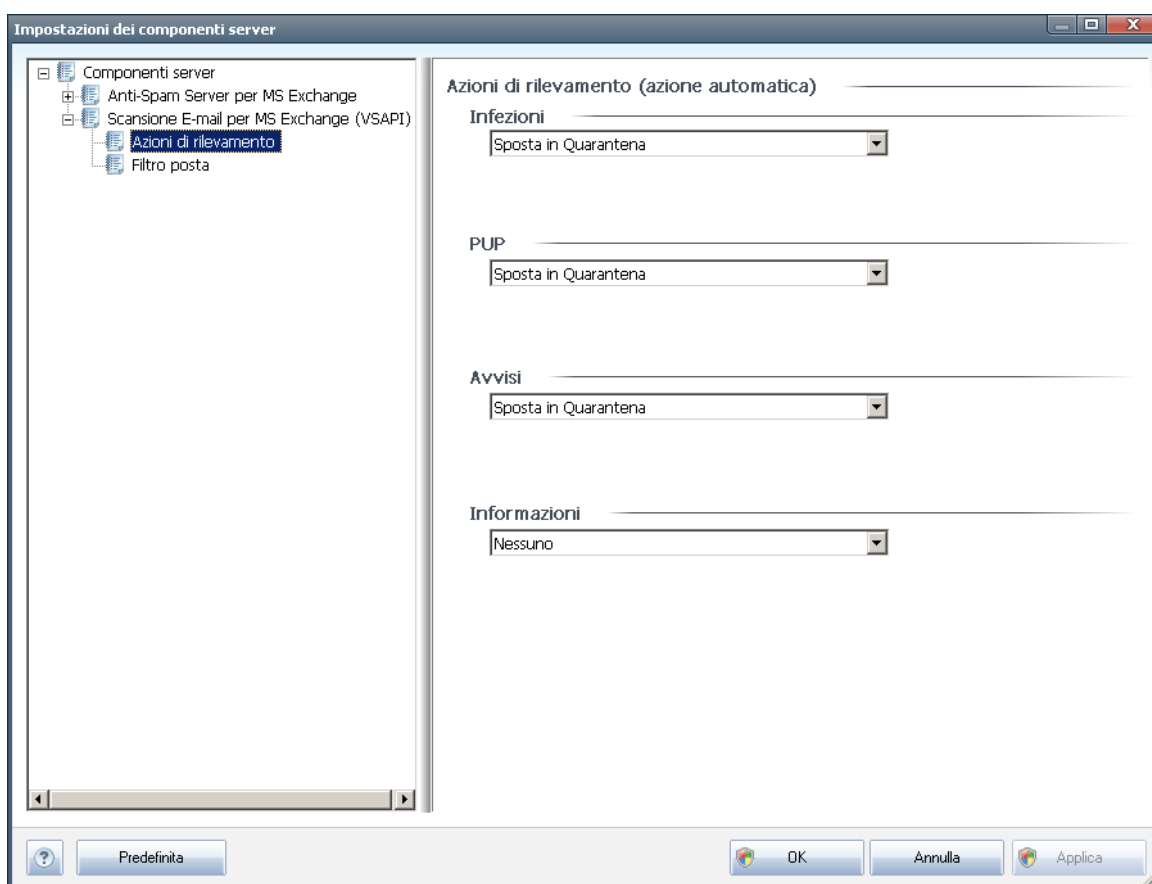
In genere, tutte queste funzioni sono estensioni per l'utente dei servizi dell'interfaccia applicativa Microsoft VSAPI 2.0/2.5. Per informazioni dettagliate su VSAPI 2.0/2.5, vedere i seguenti collegamenti e i collegamenti accessibili tramite essi:

- <http://support.microsoft.com/default.aspx?scid=kb;en-us;328841&Product=exch2k> per informazioni sull'interazione tra il software antivirus e Exchange
- <http://support.microsoft.com/default.aspx?scid=kb;en-us;823166> per

informazioni sulle funzionalità aggiuntive di VSAPI 2.5 in Exchange 2003 Server. Sono inoltre disponibili le presenti sottovoci nella seguente struttura:

- [**Azioni di rilevamento**](#)
- [**Filtro posta**](#)

5.3. Azioni di rilevamento



Nella sottovoce **Azioni di rilevamento** è possibile selezionare le azioni automatiche da eseguire durante il processo di scansione.

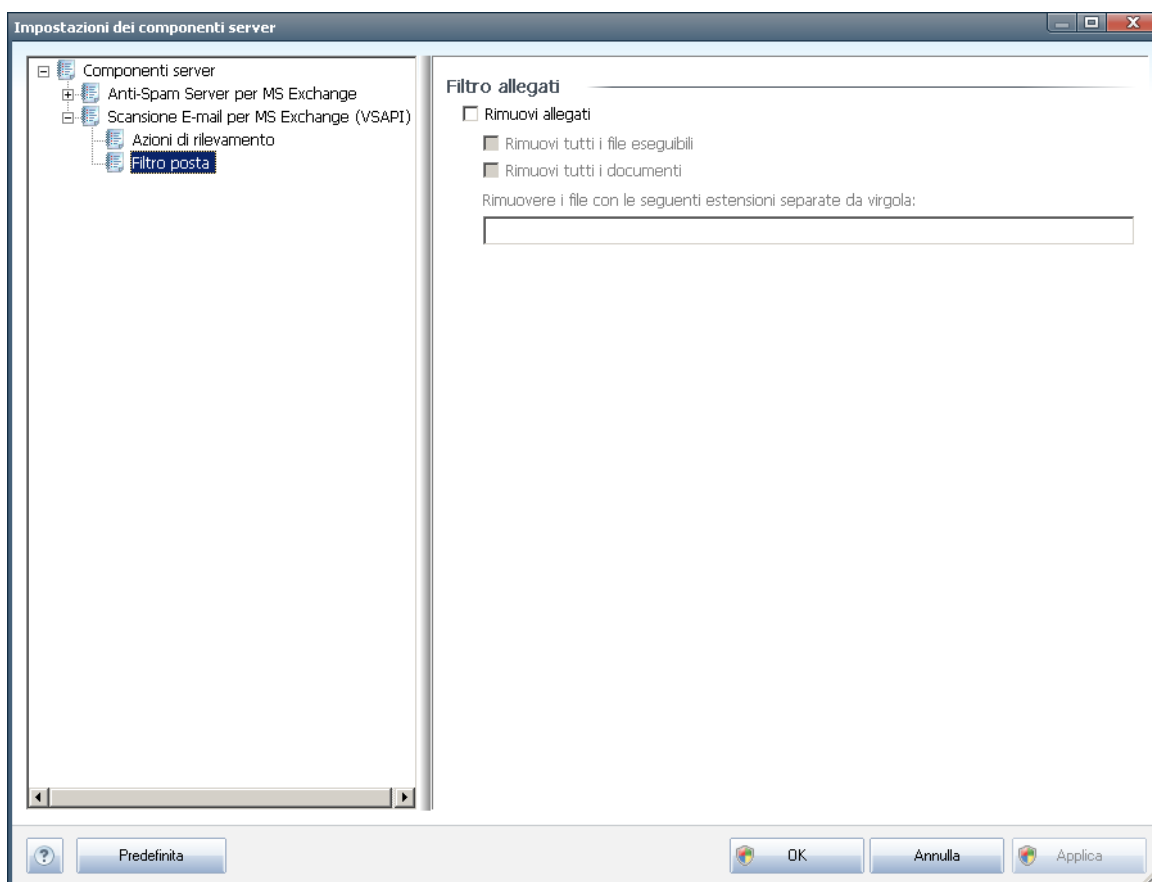
Tali azioni sono disponibili per le seguenti voci:

- **Infezioni**
- **Programmi potenzialmente indesiderati (PUP, Potentially Unwanted Programs)**
- **Avvisi**
- **Informazioni**

Utilizzare il menu a discesa per selezionare un'azione per ciascuna voce:

- **Nessuna** - non verrà eseguita nessuna azione.
- **Sposta in Quarantena** - la minaccia verrà spostata in Quarantena virus.
- **Rimuovi** - la minaccia verrà rimossa.

5.4. Filtro posta



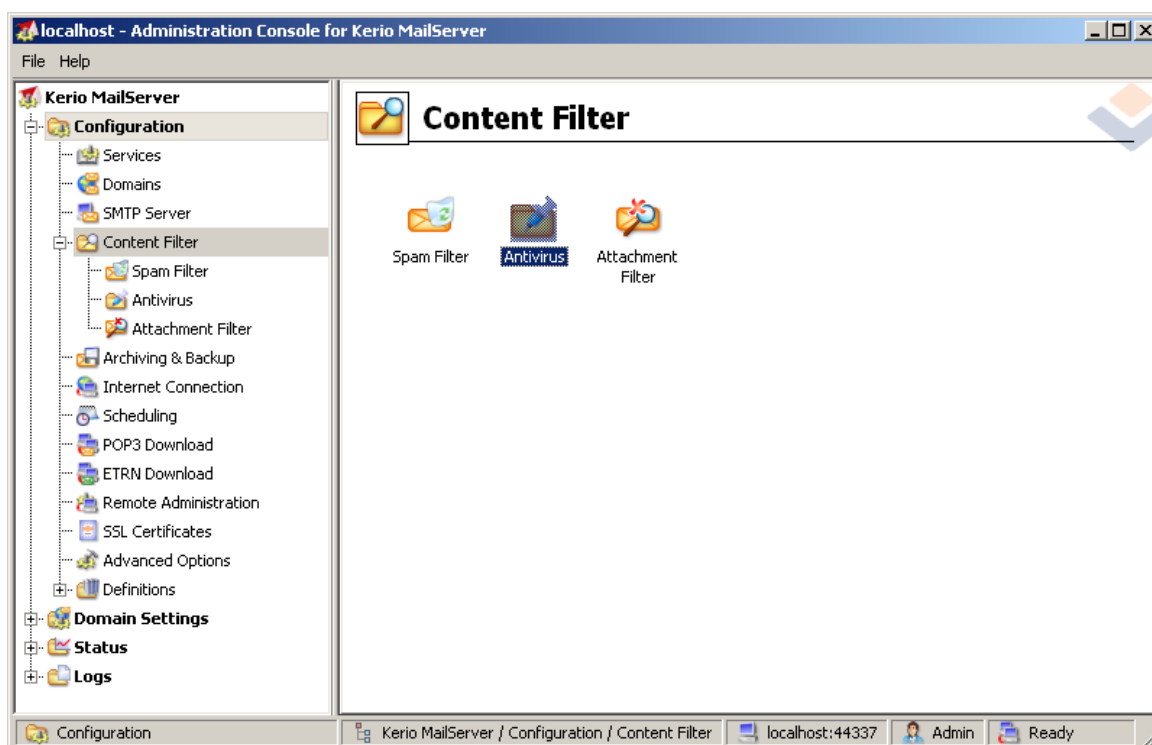
Nella sottovoce **Filtro posta** è possibile selezionare gli eventuali allegati da rimuovere automaticamente. Sono disponibili le seguenti opzioni:

- **Rimuovi allegati** - selezionare questa casella per abilitare la funzione.
- **Rimuovi tutti i file eseguibili** - consente di rimuovere tutti i file eseguibili.
- **Rimuovi tutti i documenti** - consente di rimuovere tutti i documenti.
- **Rimuovere i file con le seguenti estensioni separate da virgola** - selezionare le caselle con le estensioni che si desidera rimuovere automaticamente. Separare le estensioni con una virgola.

6. AVG per Kerio MailServer

6.1. Configurazione

Il meccanismo di protezione antivirus è integrato direttamente nell'applicazione Kerio MailServer. Per attivare la protezione dei messaggi e-mail di Kerio MailServer da parte del motore di scansione di AVG, avviare l'applicazione Kerio Administration Console. Nella struttura dei controlli nel lato sinistro della finestra dell'applicazione scegliere il ramo Filtro contenuti nel ramo Configurazione:

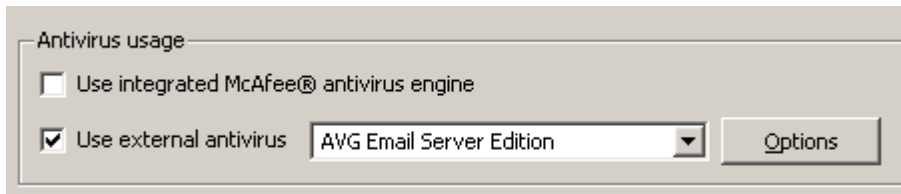


Se si fa clic su Filtro contenuti viene visualizzata la finestra di dialogo con i tre elementi:

- **Filtro spam**
- **Antivirus** (vedere la sezione **Antivirus**)
- **Filtro allegati** (vedere la sezione **Filtro allegati**)

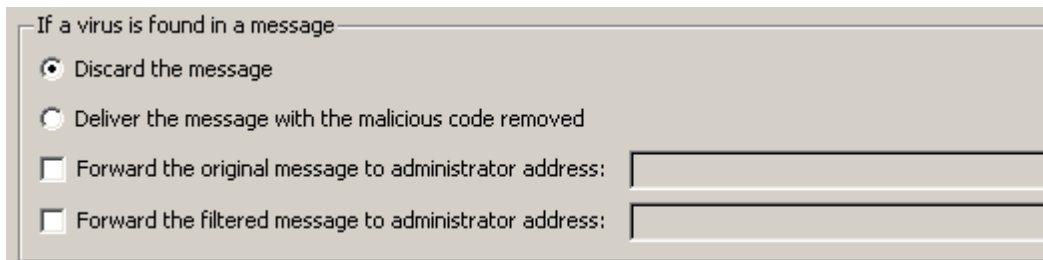
6.1.1. Antivirus

Per attivare AVG per Kerio MailServer, selezionare la casella di controllo Usa antivirus esterno e scegliere la voce AVG Email Server Edition dal menu del software esterno nel frame Uso antivirus della finestra di configurazione:



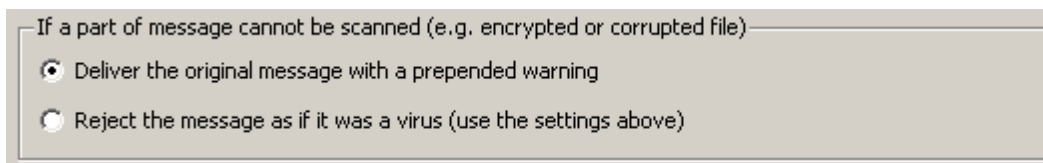
Nella seguente sezione è possibile specificare l'azione da eseguire con un messaggio infetto o filtrato:

- ***Se viene rilevato un virus in un messaggio***



Questo frame consente di specificare l'azione da eseguire quando viene rilevato un virus in un messaggio, oppure quando un messaggio viene filtrato da un filtro allegati:

- ***Elimina il messaggio***: se selezionato, il messaggio infetto o filtrato viene eliminato.
 - ***Invia il messaggio senza il codice dannoso***: se selezionato, il messaggio viene inviato al destinatario senza l'allegato potenzialmente dannoso.
 - ***Inoltra il messaggio originale all'indirizzo dell'amministratore***: se selezionato, il messaggio infetto da virus viene inoltrato all'indirizzo specificato nel campo di testo dell'indirizzo.
 - ***Inoltra il messaggio filtrato all'indirizzo dell'amministratore***: se selezionato, il messaggio filtrato viene inoltrato all'indirizzo specificato nel campo di testo dell'indirizzo.
- ***Se non è possibile esaminare una parte del messaggio (ad esempio nel caso di un file crittografato o danneggiato)***

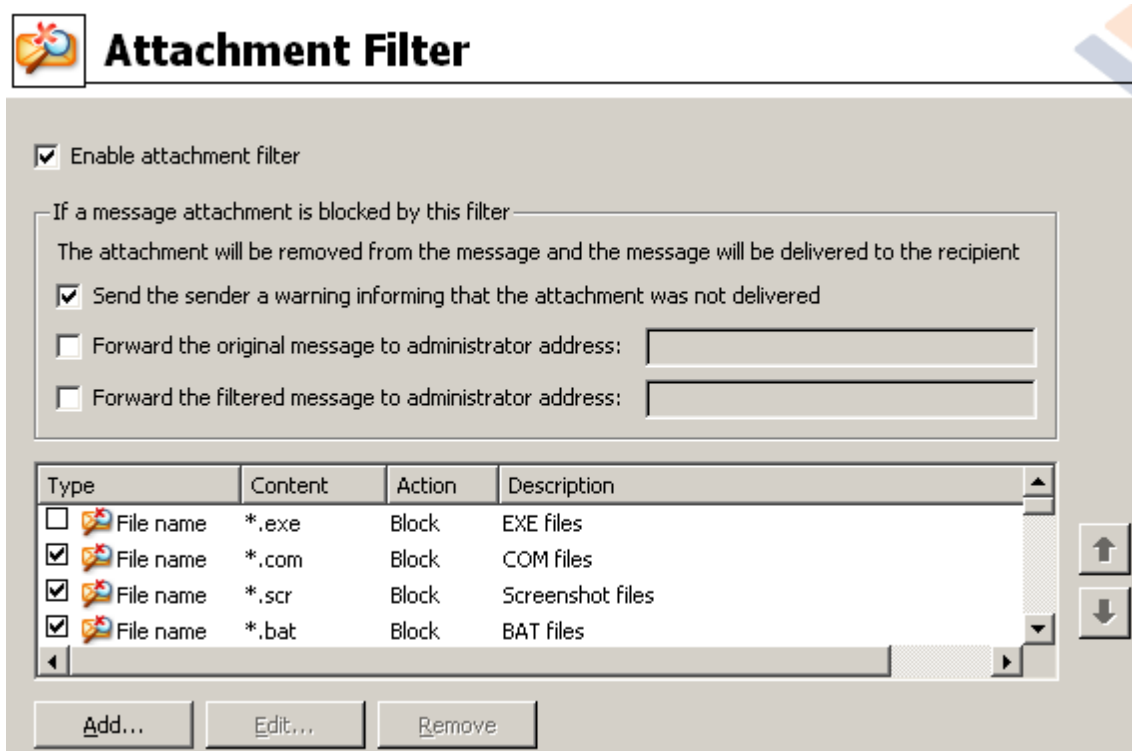


Questo frame consente di specificare l'azione da eseguire se non è possibile esaminare una parte del messaggio o dell'allegato:

- **Invia il messaggio originale con un avviso preparato:** il messaggio o l'allegato viene inviato senza essere controllato. L'utente viene avvisato che il messaggio potrebbe ancora contenere virus.
- **Rifiuta il messaggio come se fosse un virus:** il sistema si comporta come se avesse rilevato un virus (ad esempio, il messaggio viene inviato senza allegati oppure rifiutato). Questa opzione è sicura, ma l'invio di archivi protetti da password sarà virtualmente impossibile.

6.1.2. Filtro allegati

Nel menu Filtro allegati è presente un elenco di varie definizioni degli allegati:



È possibile attivare o disattivare il filtro degli allegati e-mail selezionando la casella di controllo Attiva filtro allegati. Facoltativamente, è possibile modificare le seguenti impostazioni:

- **Invia al mittente un avviso che informa che l'allegato non è stato consegnato**

Il mittente riceverà un avviso da Kerio MailServer, che informa che è stato inviato un messaggio con un allegato infetto da virus o bloccato.

- **Inoltra il messaggio originale all'indirizzo dell'amministratore**

Il messaggio verrà inoltrato (allo stato originale, ovvero con l'allegato infetto o vietato) a un indirizzo e-mail specificato, indipendentemente dal fatto che

l'indirizzo sia esterno o locale.

- **Inoltra il messaggio filtrato all'indirizzo dell'amministratore**

Il messaggio viene inviato all'indirizzo e-mail specificato senza l'allegato infetto o vietato (tranne nel caso delle azioni specificate di seguito). È possibile utilizzare questa opzione per verificare il corretto funzionamento dell'antivirus e/o del filtro degli allegati.

Nell'elenco delle estensioni, ciascuna voce dispone di quattro campi:

- **Tipo:** specifica del tipo di allegato determinato dall'estensione fornita nel campo Contenuto. I tipi possibili sono Nome file o Tipo MIME. È possibile selezionare la relativa casella in questo campo per includere o escludere la voce dal filtro degli allegati.
- **Contenuto:** consente di specificare un'estensione da filtrare. È possibile utilizzare i caratteri jolly del sistema operativo (ad esempio, la stringa "*.doc.*" rappresenta i file con estensione .doc e qualsiasi altra estensione che la segue).
- **Azione:** consente di definire le azioni da eseguire con l'allegato specifico. Le azioni possibili sono Accetta (per accettare l'allegato) e Blocca (verrà eseguita l'azione definita sopra l'elenco degli allegati non consentiti).
- **Descrizione:** la descrizione dell'allegato viene specificata in questo campo.

Facendo clic sul pulsante Rimuovi viene rimossa una voce dall'elenco. È possibile aggiungere un'altra voce all'elenco facendo clic sul pulsante **Aggiungi**. Altrimenti, è possibile modificare un record esistente facendo clic sul pulsante **Modifica**. Viene visualizzata la finestra seguente:



- Nel campo Descrizione è possibile scrivere una breve descrizione dell'allegato da filtrare.

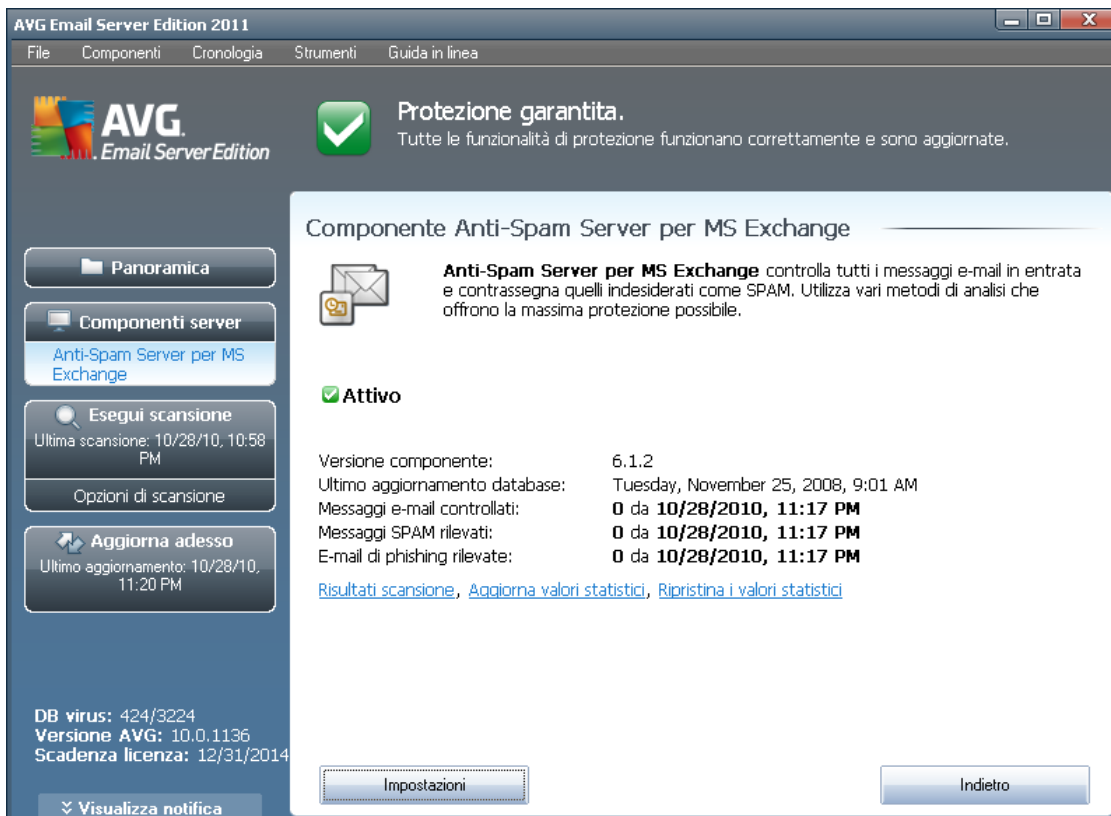


- Nel campo Se un messaggio di posta contiene un allegato in cui, è possibile selezionare il tipo di allegato (Nome file o Tipo MIME). È inoltre possibile scegliere un'estensione specifica dall'elenco delle estensioni disponibili oppure digitare direttamente il carattere jolly dell'estensione.

Nel campo Quindi è possibile decidere se bloccare o accettare l'allegato specificato.

7. Configurazione dell'Anti-Spam

7.1. Interfaccia dell'Anti-Spam



The screenshot shows the AVG Email Server Edition 2011 interface. The main window title is "AVG Email Server Edition 2011". The menu bar includes "File", "Componenti", "Cronologia", "Strumenti", and "Guida in linea". The interface is divided into a left sidebar and a main content area.

Left Sidebar:

- Panoramica**
- Componenti server**
 - Anti-Spam Server per MS Exchange
- Esegui scansione**
 - Ultima scansione: 10/28/10, 10:58 PM
 - Opzioni di scansione
- Aggiorna adesso**
 - Ultimo aggiornamento: 10/28/10, 11:20 PM

Main Content Area:

Protezione garantita.
Tutte le funzionalità di protezione funzionano correttamente e sono aggiornate.

Componente Anti-Spam Server per MS Exchange

Anti-Spam Server per MS Exchange controlla tutti i messaggi e-mail in entrata e contrassegna quelli indesiderati come SPAM. Utilizza vari metodi di analisi che offrono la massima protezione possibile.

Attivo

Versione componente:	6.1.2
Ultimo aggiornamento database:	Tuesday, November 25, 2008, 9:01 AM
Messaggi e-mail controllati:	0 da 10/28/2010, 11:17 PM
Messaggi SPAM rilevati:	0 da 10/28/2010, 11:17 PM
E-mail di phishing rilevate:	0 da 10/28/2010, 11:17 PM

[Risultati scansione](#), [Aggiorna valori statistici](#), [Ripristina i valori statistici](#)

Bottom Left: DB virus: 424/3224, Versione AVG: 10.0.1136, Scadenza licenza: 12/31/2014

Buttons: Impostazioni, Indietro

La finestra di dialogo del componente server **Anti-Spam** è disponibile nella sezione **Componenti server** (menu a sinistra). Contiene brevi informazioni sulla funzionalità del componente server, informazioni sul relativo stato corrente (ad esempio *Il componente Anti-Spam Server per MS Exchange è attivo*) e alcune statistiche.

Collegamenti disponibili:

- **Risultati scansione**

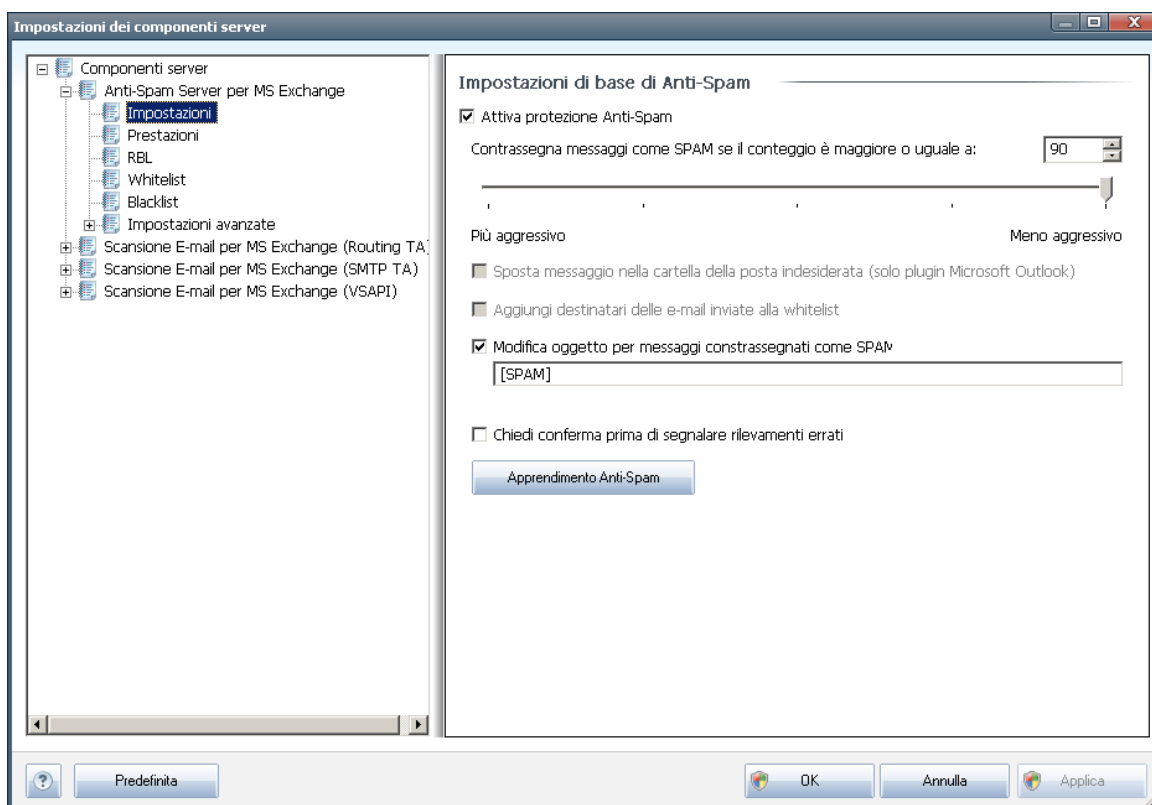
Aprire una nuova finestra di dialogo in cui è possibile visualizzare i risultati della scansione anti-spam:

7.2. Principi dell'Anti-Spam

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

Anti-Spam controlla tutti i messaggi e-mail in entrata e contrassegna quelli indesiderati come SPAM. Per elaborare ogni messaggio e-mail vengono utilizzati diversi metodi di analisi che offrono il massimo livello di protezione possibile contro i messaggi e-mail indesiderati.

7.3. Impostazioni dell'Anti-Spam



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

Nella finestra di dialogo 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 messaggi come SPAM se il conteggio è maggiore o uguale a**,



digitare un valore (*compreso tra 50 e 90*) oppure spostare il dispositivo di scorrimento a destra o a sinistra.

Di seguito viene fornita una panoramica generale della soglia di conteggio:

- **Valore 90:** la maggior parte dei messaggi e-mail in entrata verrà recapitata normalmente (senza venire contrassegnata come [spam](#)). Lo [spam](#) più facilmente identificato verrà filtrato, tuttavia si potrebbe ricevere comunque una notevole quantità di [spam](#).
- **Valore compreso tra 80 e 89:** verranno filtrati i messaggi e-mail il cui contenuto potrebbe essere [spam](#), ma potrebbero essere filtrati anche alcuni messaggi che non ne contengono.
- **Valore compreso tra 60 e 79:** è considerata una configurazione piuttosto aggressiva. Verranno filtrati i messaggi e-mail il cui contenuto può essere [spam](#), ma potrebbero essere filtrati anche messaggi che non ne contengono.
- **Valore compreso tra 50 e 59:** configurazione particolarmente aggressiva. È probabile che insieme ai messaggi e-mail contenenti [spam](#) vengano filtrati anche i messaggi normali. Questo intervallo di valori non è consigliato per l'uso normale.

È possibile definire ulteriormente il modo in cui trattare i messaggi e-mail di [spam](#) rilevati:

- **Modifica oggetto per messaggi contrassegnati come spam:** selezionare questa casella di controllo se si desidera che tutti i messaggi rilevati come [spam](#) vengano contrassegnati con una parola o un carattere specifico nel campo dell'oggetto del messaggio e-mail; il testo desiderato può essere digitato nel campo di testo attivato.
- **Chiedi conferma prima di segnalare rilevamenti errati:** se durante il processo di installazione si è scelto di partecipare al Programma di miglioramento del prodotto (questo programma ci consente di raccogliere informazioni aggiornate fornite da tutti gli utenti in tutto il mondo sulle minacce più recenti e di migliorare la protezione in rete per tutti), ossia si è acconsentito a segnalare le minacce rilevate a AVG. La segnalazione viene effettuata automaticamente. Tuttavia, è possibile selezionare questa casella di controllo per specificare che si desidera venga richiesta una conferma prima che eventuale spam rilevato venga segnalato a AVG, in modo da assicurarsi che il messaggio possa effettivamente essere classificato come spam.

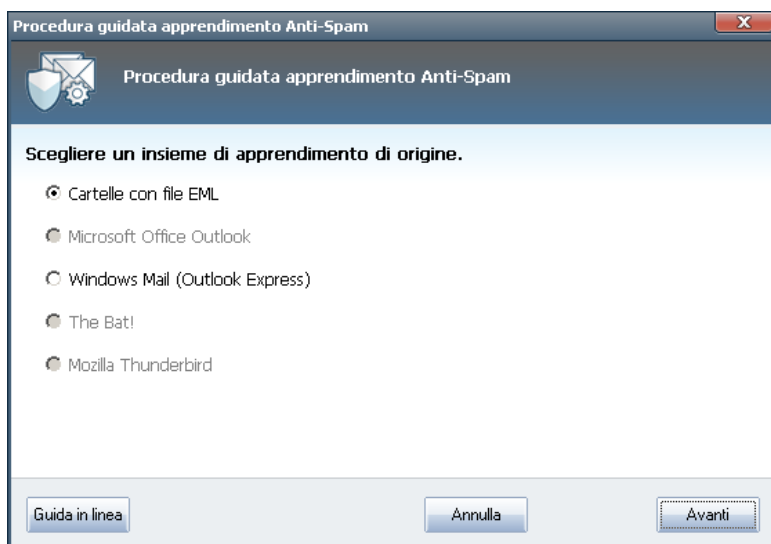
Nota: questa opzione non è applicabile a AVG Email Server Edition 2011.

Il pulsante **Apprendimento anti-spam** consente di aprire la [Procedura guidata apprendimento anti-spam](#) descritta dettagliatamente nel [capitolo successivo](#).

7.3.1. Procedura guidata apprendimento anti-spam

Nella prima finestra di dialogo della **Procedura guidata apprendimento anti-spam** viene richiesto di selezionare l'origine dei messaggi e-mail da utilizzare per l'apprendimento. Di norma, si utilizzeranno messaggi e-mail erroneamente

contrassegnati come SPAM o messaggi di spam che non sono stati riconosciuti.



Sono disponibili le seguenti opzioni:

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

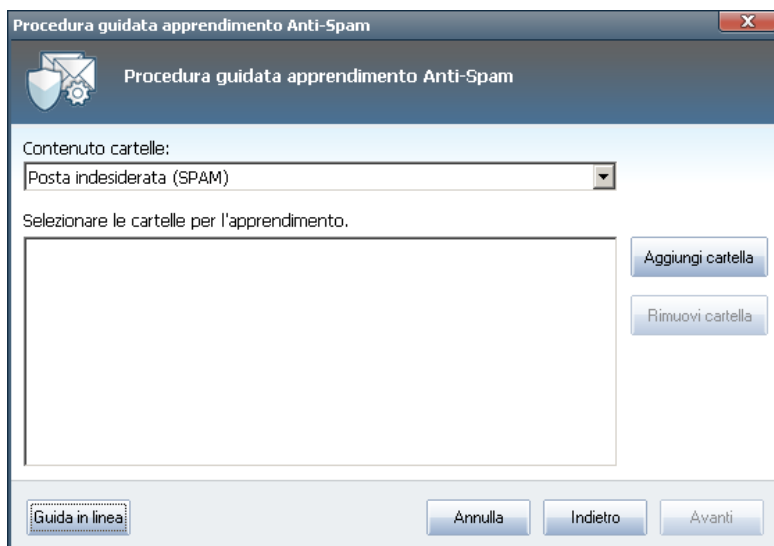
Per un processo di apprendimento più semplice e rapido, è innanzitutto consigliabile ordinare i messaggi e-mail nelle cartelle, in modo che la cartella utilizzata per l'apprendimento contenga solo i messaggi per l'apprendimento (desiderati o indesiderati). Questa operazione non è tuttavia indispensabile,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

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

7.3.2. Seleziona cartella con messaggi

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

Cartelle con file EML



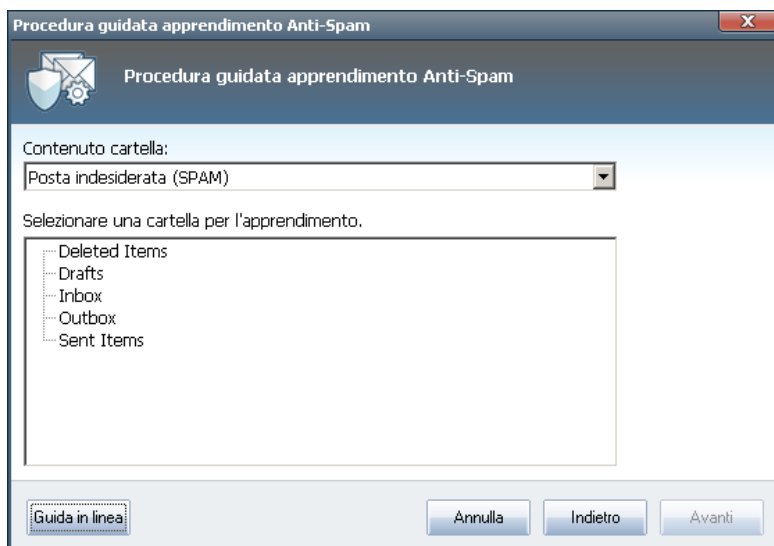
In questa finestra di dialogo selezionare la cartella contenente i messaggi che si desidera utilizzare per l'apprendimento. Fare clic sul pulsante **Aggiungi cartella** per individuare la cartella con i file .eml (*messaggi e-mail salvati*). La cartella selezionata verrà visualizzata nella finestra di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

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

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

Client e-mail specifico

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

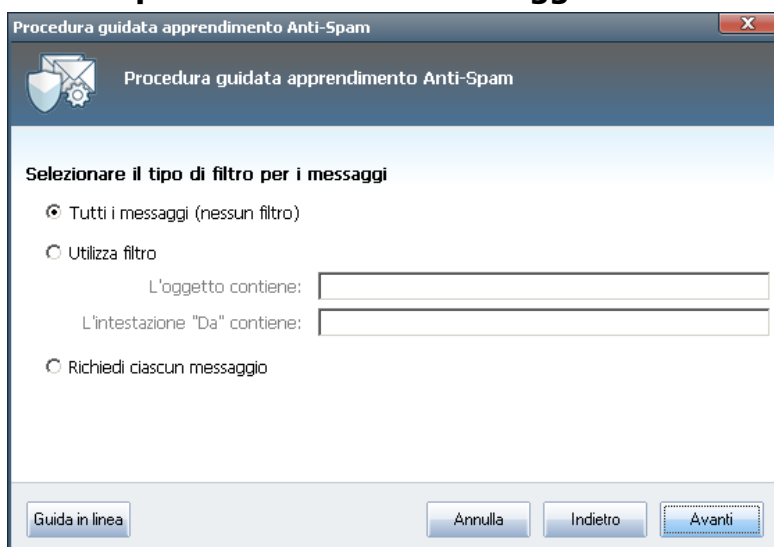


Nota: se si utilizza Microsoft Outlook, verrà richiesto innanzitutto di selezionare il profilo di MS Outlook.

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

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

7.3.3. Opzioni di filtro dei messaggi





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

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

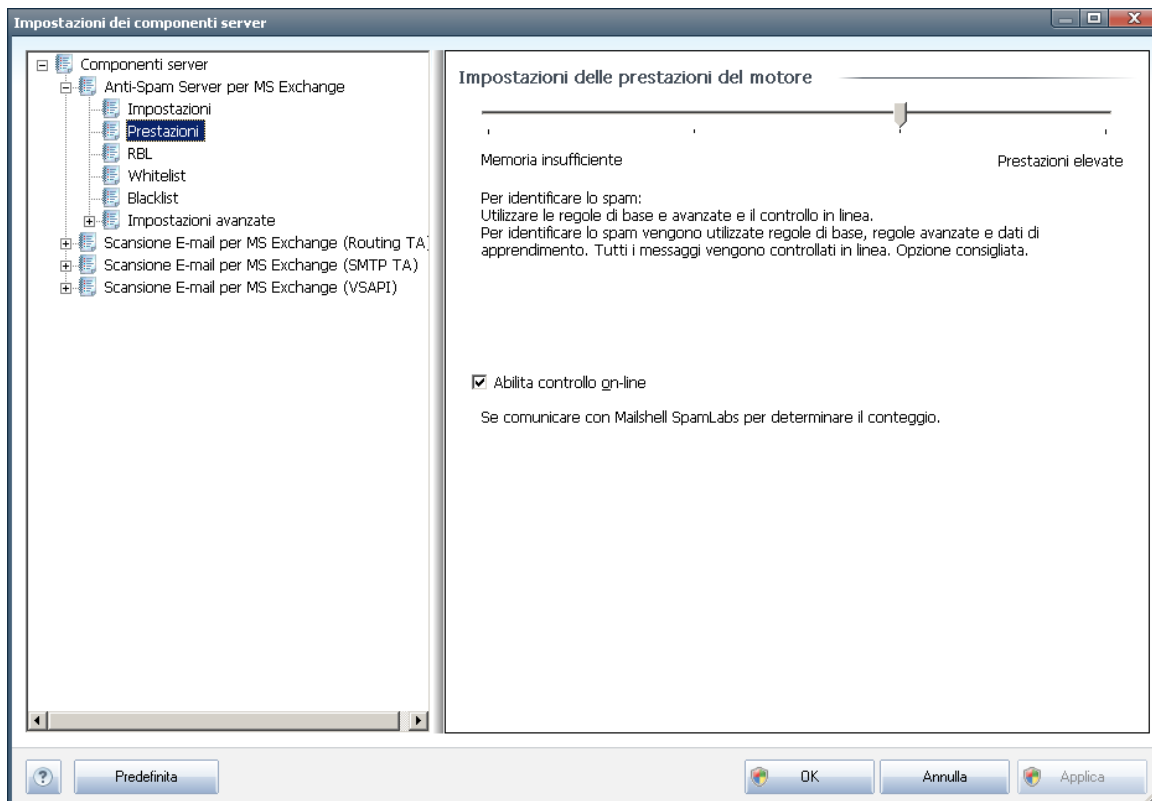
Se si hanno dubbi sui messaggi contenuti nella cartella e si desidera che durante la procedura guidata venga richiesta una conferma per ogni singolo messaggio (al fine di determinare se utilizzarlo o meno per l'apprendimento), selezionare l'opzione **Chiedi per ogni messaggio**.

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

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

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

7.4. Prestazioni



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

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

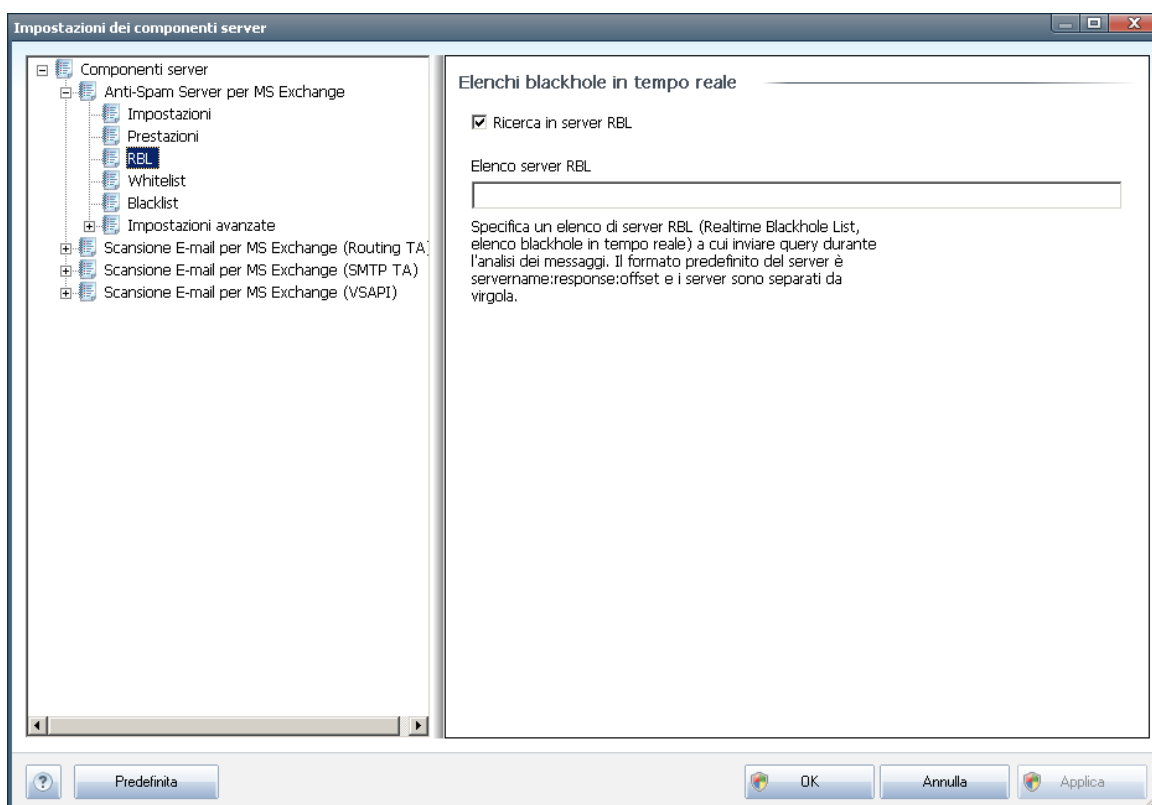
La voce **Abilita controllo on-line** è attiva per impostazione predefinita. Ne risulta un rilevamento dello [spam](#) più preciso tramite la comunicazione con i server [Mailshell](#), ovvero i dati sottoposti a scansione verranno confrontati con i database [Mailshell](#) in linea.

In genere si consiglia di mantenere le impostazioni predefinite e di modificarle solo se esiste un reale motivo per farlo. Le eventuali modifiche alla

configurazione devono essere eseguite solo da utenti esperti.

7.5. RBL

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



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

Il server RBL (*Realtime Blackhole List, Elenchi blackhole in tempo reale*) è un server DNS con un vasto database di mittenti di spam noti. Se questa funzione è attivata, tutti i messaggi e-mail verranno verificati in base al database del server RBL e verranno contrassegnati come [spam](#) se risulteranno identici a una delle voci nel database.

I database dei server RBL contengono le impronte digitali di spam più aggiornate, per fornire il rilevamento di [spam](#) migliore e più accurato. La funzione è particolarmente utile per gli utenti che ricevono grandi quantità di messaggi di spam normalmente non rilevati dal motore Anti-Spam.

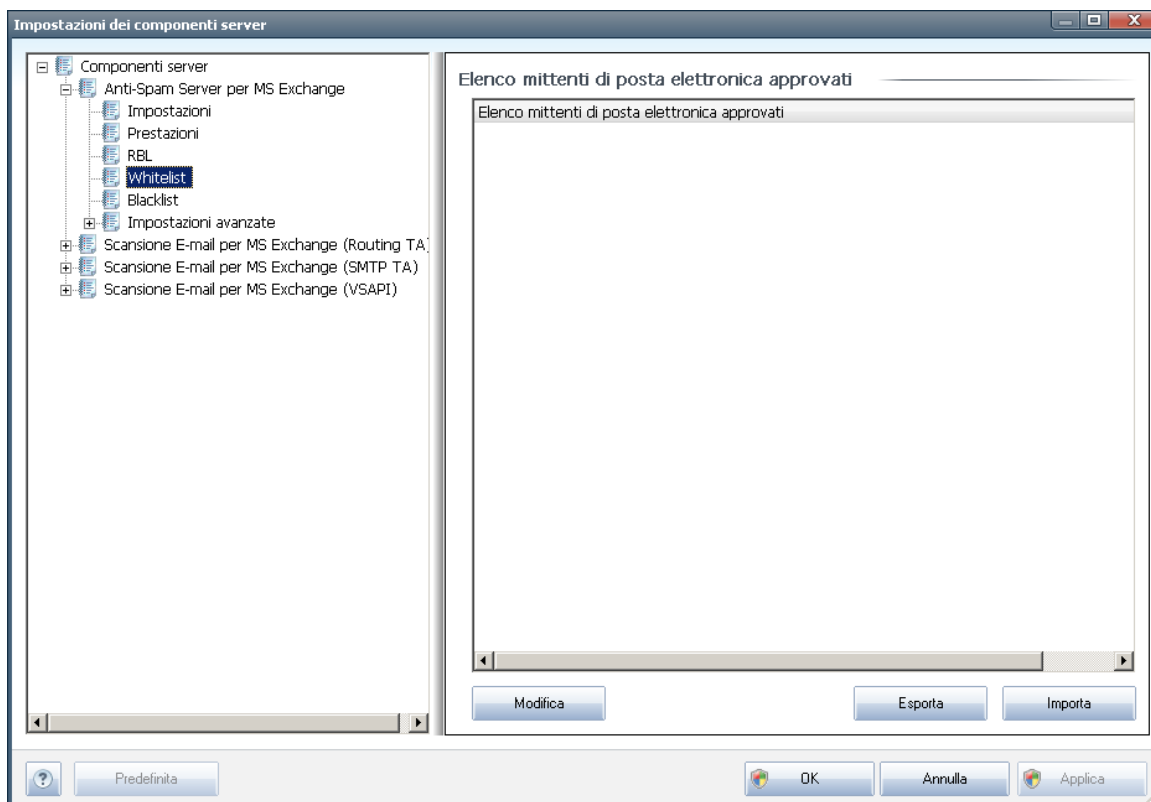
La funzione **Elenco server RBL** consente di definire le posizioni dei server RBL specifici. Per impostazione predefinita, sono specificati due indirizzi server RBL. Se non si è utenti esperti e non si necessita realmente di modificare queste impostazioni, si consiglia di mantenere le impostazioni predefinite.

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

Non vengono inviati dati personali al server.

7.6. Whitelist

La voce **Whitelist** consente di aprire una finestra di dialogo con un elenco globale di indirizzi di mittenti e-mail e nomi di dominio 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 genereranno mai messaggi di spam.

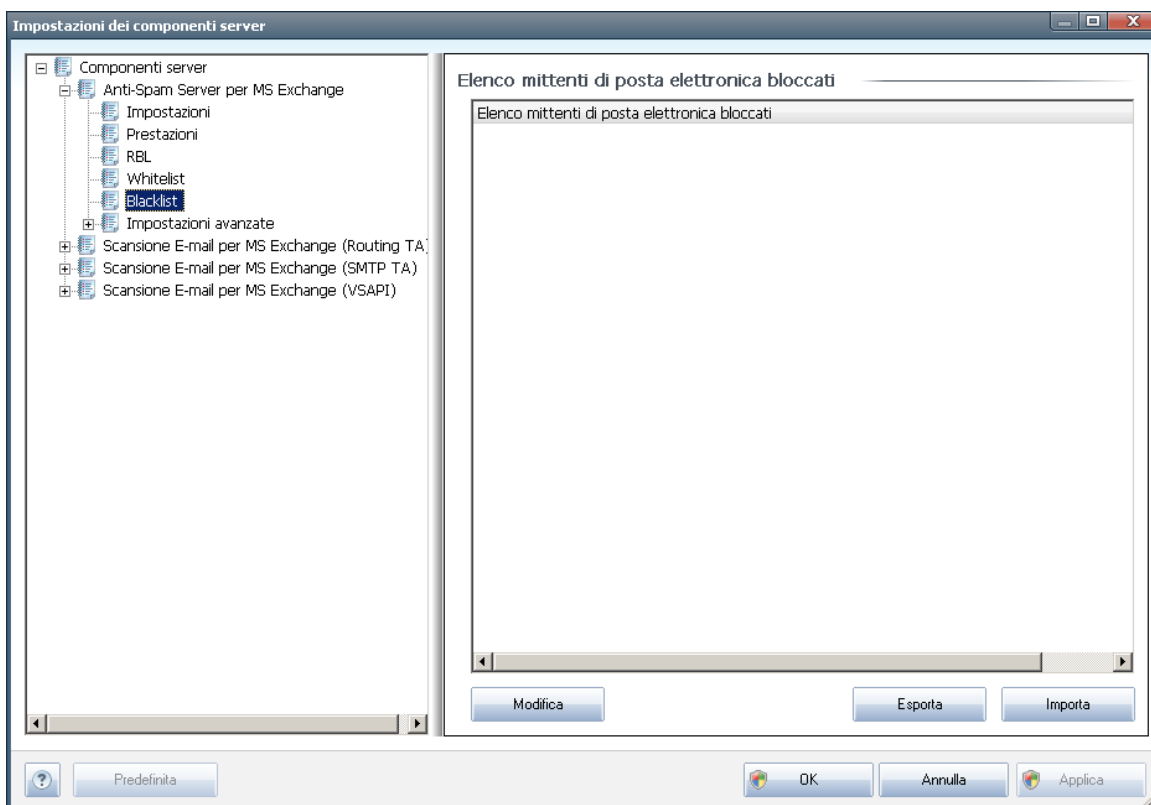
Dopo che è stato preparato l'elenco di mittenti e/o nomi di dominio, è possibile inserirli in due modi diversi: immettendo direttamente ciascun indirizzo e-mail o importando tutto l'elenco di indirizzi. Sono disponibili i seguenti pulsanti di controllo:

- **Modifica:** selezionare questo pulsante per aprire una finestra di dialogo in cui è possibile immettere manualmente un elenco di indirizzi (è inoltre possibile utilizzare il metodo *copia e incolla*). Immettere una voce (mittente o nome di dominio) per riga.

- **Importa:** è possibile importare gli indirizzi e-mail esistenti selezionando questo pulsante. Il file di input può essere un file di testo (in formato testo normale, e il contenuto deve includere solo una voce - indirizzo, nome di dominio - per riga) o un file WAB oppure l'importazione può essere eseguita dalla Rubrica di Windows o da Microsoft Outlook.
- **Esporta:** se per qualsiasi motivo si decide di esportare i record, è possibile fare clic su questo pulsante per eseguire l'operazione. Tutti i record verranno salvati in un file di testo normale.

7.7. Blacklist

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



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

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



- **Modifica:** selezionare questo pulsante per aprire una finestra di dialogo in cui è possibile immettere manualmente un elenco di indirizzi (è inoltre possibile utilizzare il metodo *copia e incolla*). Immettere una voce (mittente o nome di dominio) per riga.
- **Importa:** è possibile importare gli indirizzi e-mail esistenti selezionando questo pulsante. Il file di input può essere un file di testo (in formato testo normale, e il contenuto deve includere solo una voce - indirizzo, nome di dominio - per riga) o un file WAB oppure l'importazione può essere eseguita dalla Rubrica di Windows o da Microsoft Outlook.
- **Esporta:** se per qualsiasi motivo si decide di esportare i record, è possibile fare clic su questo pulsante per eseguire l'operazione. Tutti i record verranno salvati in un file di testo normale.

7.8. Impostazioni avanzate

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.

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 descrizione relativa è sempre inclusa nella finestra di dialogo:

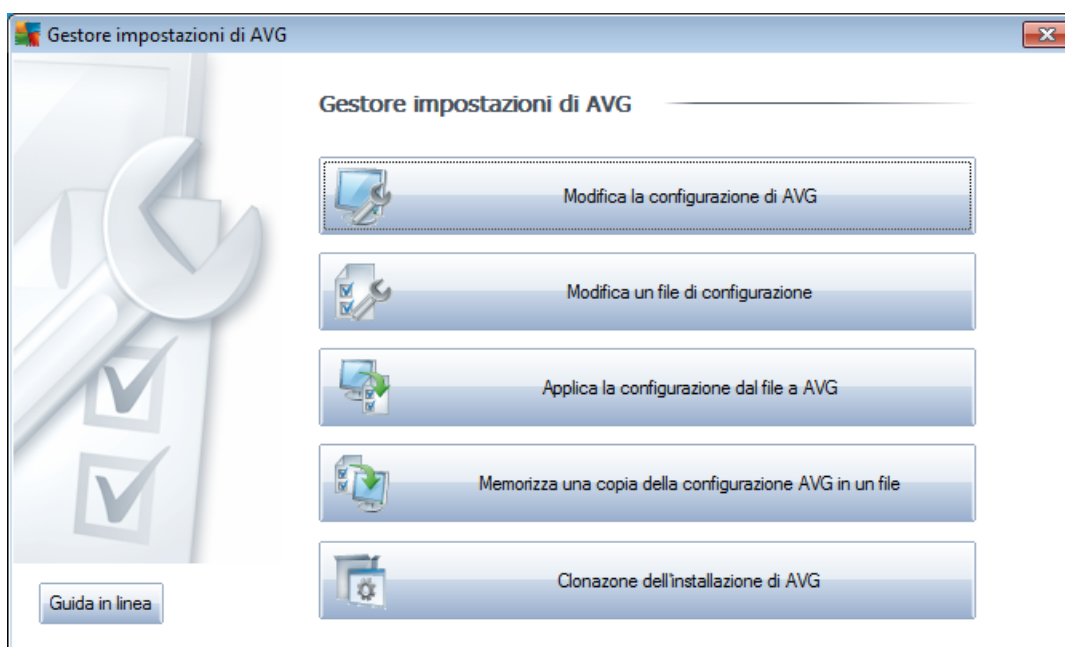
- **Cache:** impronte digitali, reputazione dominio, LegitRepute
- **Apprendimento:** numero massimo di parole, soglia di apprendimento automatico, peso
- **Filtraggio:** elenco lingue, elenco paesi, IP approvati, IP bloccati, paesi bloccati, set di caratteri bloccati, mittenti contraffatti
- **RBL:** server RBL, multihit, soglia, timeout, massimo IP
- **Connessione Internet:** timeout, server proxy, autenticazione server proxy

8. AVG Settings Manager

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

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

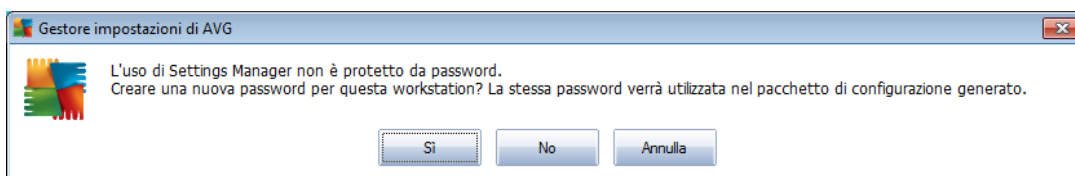
Tutti i programmi/AVG 2011/AVG Settings Manager



- **Modifica la configurazione AVG di questo computer**
Utilizzare questo pulsante per aprire una finestra di dialogo con le impostazioni avanzate dell'installazione AVG locale. Tutte le modifiche apportate qui verranno applicate inoltre all'installazione AVG locale.
- **Carica e modifica il file di configurazione di AVG**
Se si dispone già di un file di configurazione di AVG (.pck), utilizzare questo pulsante per aprire il file per la modifica. Dopo aver confermato le modifiche tramite il pulsante **OK** o **Applica**, il file conterrà le nuove impostazioni.
- **Applica configurazione dal file a AVG su questo computer**
Utilizzare questo pulsante per aprire un file di configurazione di AVG (.pck) e applicarlo all'installazione locale di AVG.
- **Memorizza la configurazione AVG locale in un file**



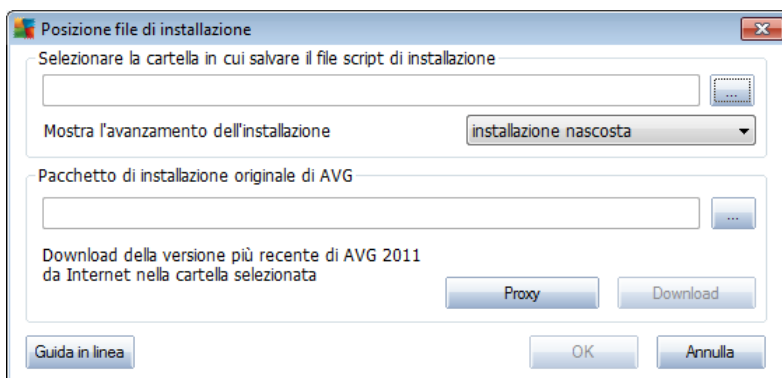
Utilizzare questo pulsante per salvare il file di configurazione di AVG (.pck) dell'installazione locale di AVG. Se non è stata impostata una password per le azioni consentite, potrebbe venire visualizzata la seguente finestra di dialogo:



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

- **Clona installazione AVG**

Questa opzione consente di ottenere una copia esatta dell'installazione AVG locale creando un pacchetto di installazione con opzioni personalizzate. Per procedere selezionare innanzitutto la cartella in cui salvare lo script di installazione.



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

- **Installazione nascosta:** non verrà visualizzata alcuna informazione durante il processo di installazione.
- **Mostra l'avanzamento dell'installazione:** l'installazione non richiederà alcun intervento da parte dell'utente, ma l'avanzamento sarà completamente visibile.
- **Mostra l'installazione guidata:** l'installazione sarà visibile e l'utente dovrà confermare manualmente tutti i passaggi.

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



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

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



9. Domande frequenti e assistenza tecnica

Se si verificano problemi con AVG, di tipo commerciale o tecnico, fare riferimento alla sezione delle **Domande frequenti** del sito Web di AVG all'indirizzo <http://www.avg.com>.

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