AVG 9.0 Email Server Edition

Manuale per l'utente

Revisione documento 90.1 (5. 9. 2009)

Sommario

1. Introduzione

Il presente manuale per l'utente fornisce una documentazione completa per **AVG 9.0 Email Server Edition**.

Congratulazioni per l'acquisto di AVG 9.0 Email Server Edition.

AVG 9.0 Email Server Edition è la gamma di prodotti AVG pluripremiati progettata per fornire maggiore tranquillità e la protezione completa del PC. Analogamente a tutti i prodotti AVG, **AVG 9.0 Email Server Edition** 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 del computer e della rete. Goditi l'esperienza della protezione completa offerta da AVG.

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/it.*

2. Requisiti per l'installazione di AVG

2.1. Sistemi operativi supportati

AVG 9.0 Email Server Edition consente di proteggere i server e-mail in esecuzione con i seguenti sistemi operativi:

- Windows 2008 Server Edition (x86 e x64)
- Windows 2003 Server (x86, x64 e Itanium) SP1
- Windows 2000 Server SP4 + Update Rollup 1

2.2. Server e-mail supportati

Sono supportati i seguenti server e-mail:

- ***Versione MS Exchange 2000 Server (con Service Pack 1 o superiore)***

  Nota: per Exchange 2000 Server il Service Pack 1 (o superiore) deve essere applicato prima di utilizzare il motore AVG; **AVG per MS Exchange 2000/2003 Server** utilizza l'interfaccia dell'applicazione VSAPI 2.0 (o 2.5 con Exchange 2003 Server) coperta in questo Service Pack.

- ***Versione MS Exchange 2003 Server***
- ***Versione MS Exchange 2007 Server***
- ***AVG per Kerio MailServer*** – versione 5.x/6.x e successive

2.3. Requisiti hardware

I requisiti hardware minimi per **AVG 9.0 Email Server Edition** 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 9.0 Email Server Edition** 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 si dispone di una versione precedente di AVG Email Server, sarà necessario disinstallarla manualmente prima di installare **AVG 9.0 Email Server Edition**. 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.

2.5. Service Pack di MS Exchange

Poiché **AVG per MS Exchange 2000/2003 Server** utilizza l'interfaccia di scansione dei virus VSAPI 2.0/2.5, è necessario che nel sistema sia installato il Service Pack 1 (o versione successiva) di MS Exchange 2000 Server. Seguire il collegamento sottostante per ottenere il Service Pack più recente di MS Exchange 2000 Server:

Service Pack per MS Exchange 2000 Server:

http://www.microsoft.com/technet/prodtechnol/exchange/downloads/2000/sp3/default.mspx

Per MS Exchange 2003 Server non è necessario alcun Service Pack aggiuntivo; tuttavia, si consiglia di mantenere il sistema aggiornato con i Service Pack e 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.mspx

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. Verranno eliminate 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

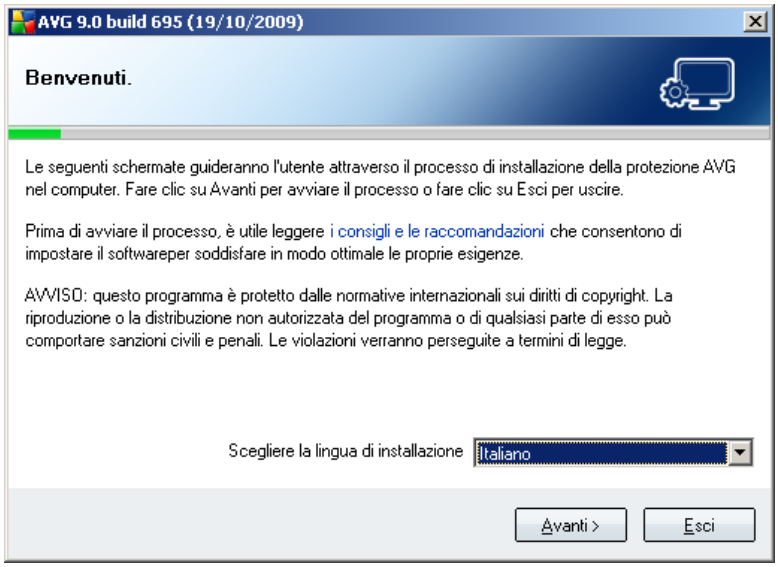
3. Processo di installazione di AVG

Per installare AVG nel computer, è bene disporre del file di installazione più recente. È possibile utilizzare il file di installazione nel CD in dotazione con il prodotto; tuttavia questo file potrebbe non essere aggiornato. Pertanto, è consigliabile procurarsi il file di installazione più recente in linea. È possibile scaricare il file dal sito Web di AVG (all'indirizzo http://www.avg.com/it/download?prd=msw).

Durante il processo di installazione verrà richiesto il numero di licenza. Prima di avviare l'installazione, assicurarsi che sia disponibile. Il numero di vendita si trova nel pacchetto del CD. Se la copia di AVG è stata acquistata via Web, il numero di licenza è stato 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 ad ogni passaggio. Di seguito viene fornita una descrizione di ciascuna finestra di dialogo:

3.1. Avvio dell'installazione



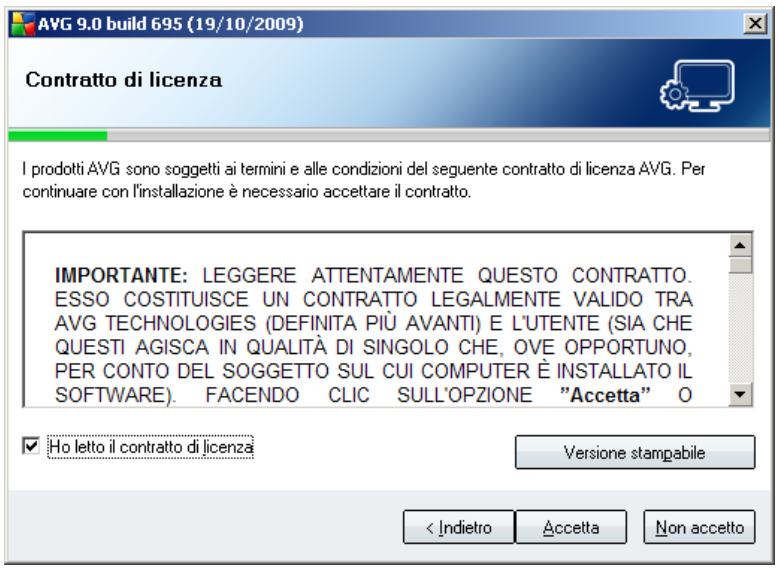
La prima finestra visualizzata del processo di installazione è quella ***introduttiva***. Da qui è possibile selezionare la lingua utilizzata per il processo di installazione. Nella parte inferiore della finestra di dialogo, individuare la voce ***Scegliere la lingua di installazione*** e selezionare la lingua desiderata dal menu a discesa. Quindi selezionare il pulsante ***Avanti*** per confermare e procedere alla finestra di dialogo successiva.

Attenzione: *in questa fase si sceglie solo la lingua per il processo di installazione. Non si sta selezionando la lingua per l'applicazione AVG, che può essere specificata successivamente durante il processo di installazione.*

3.2. Contratto di licenza

Nella finestra di dialogo ***Contratto di licenza*** è disponibile l'intero contenuto del contratto di licenza AVG. Leggere con attenzione il contratto e confermarne lettura e accettazione selezionando la casella di controllo ***Ho letto il contratto di licenza***, quindi selezionando il pulsante ***Accetto***. Se non si accettano i termini del contratto di licenza, selezionare il pulsante ***Non accetto***. Il processo di installazione verrà interrotto immediatamente.

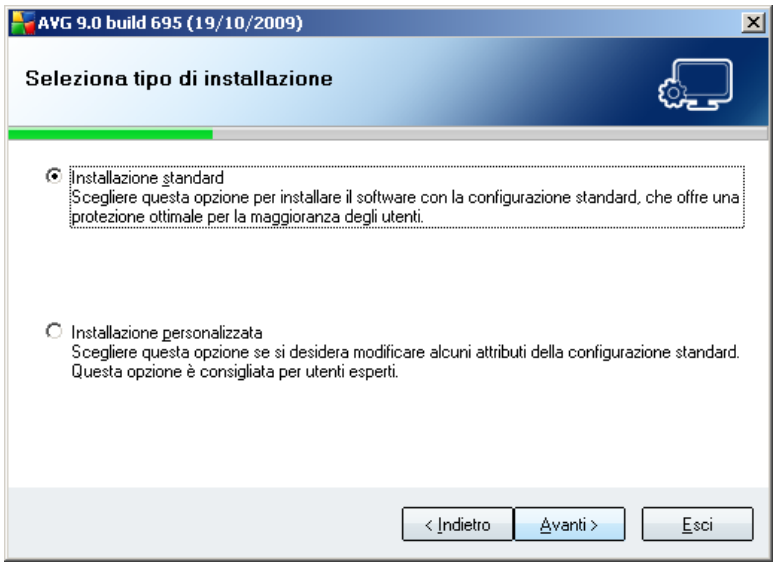
Utilizzare il pulsante ***Versione stampabile*** per aprire il contratto di licenza nell'apposita finestra destinata alla stampa.



3.3. Controllo stato del sistema in corso

Una volta accettati i termini del contratto di licenza, si verrà reindirizzati alla finestra di dialogo ***Controllo stato del sistema in corso***. Non è necessario alcun intervento dell'utente; viene eseguito un controllo del sistema prima di avviare l'installazione di AVG. Attendere il completamento del programma, quindi passare alla finestra di dialogo successiva.

3.4. Seleziona tipo di installazione



La finestra di dialogo ***Seleziona tipo di installazione*** consente di scegliere tra due opzioni di installazione: ***installazione standard*** e ***installazione personalizzata***.

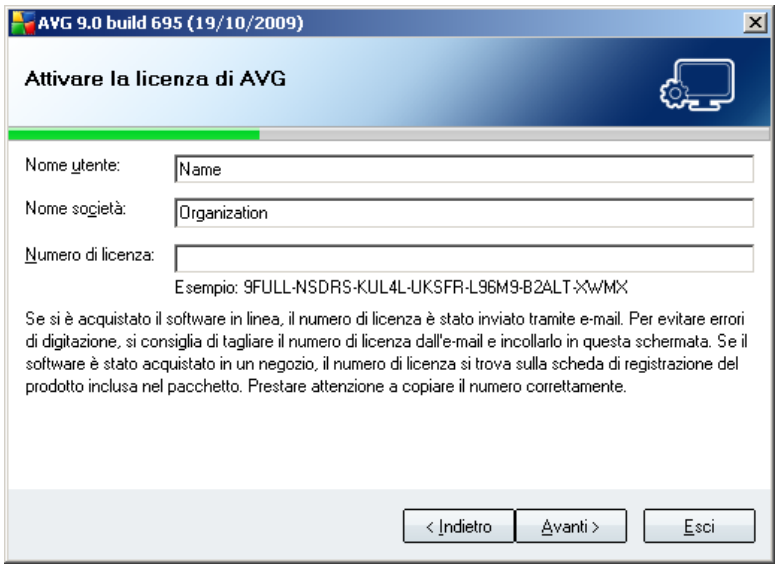
Alla maggior parte degli utenti si consiglia di mantenere l'***installazione standard***, che consente di installare AVG in modalità completamente automatica con le impostazioni predefinite dal fornitore del software. La configurazione fornisce la massima protezione combinata con l'utilizzo ottimale delle risorse. In futuro, se ci fosse necessità di modifcare 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.

3.5. Attiva AVG

Nella finestra di dialogo ***Attiva AVG*** è necessario immettere i dati di registrazione. Digitare il nome (nel campo ***Nome utente***) e il nome dell'organizzazione (nel campo ***Nome azienda).***

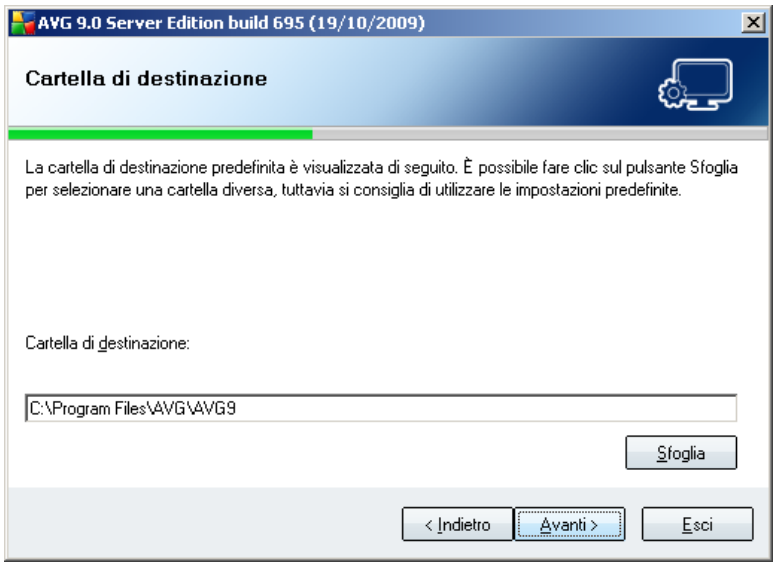
Immettere quindi il numero di licenza nel campo di testo ***Numero di licenza***. Il numero di licenza sarà contenuto nel messaggio e-mail di conferma ricevuto dopo l'acquisto in linea di AVG. È necessario digitare il numero esattamente come viene indicato. Se il numero di licenza è disponibile nel formato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



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

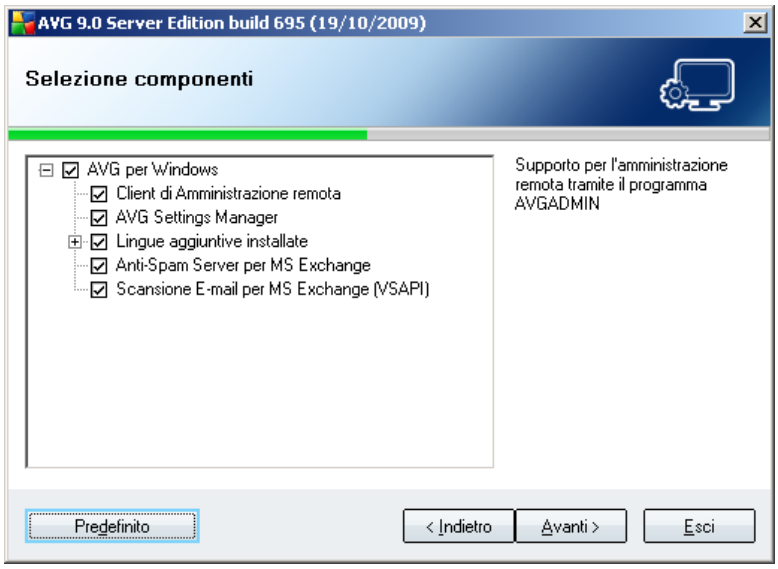
Se nel passaggio precedente è stata selezionata l'installazione standard, verrà visualizzata la finestra di dialogo ***Riepilogo installazione***. Se è stata selezionata l'installazione personalizzata, si proseguirà con la finestra di dialogo ***Cartella di destinazione***.

3.6. Installazione personalizzata - Cartella di destinazione



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

3.7. Installazione personalizzata - Selezione dei componenti



Nella finestra di dialogo ***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.

Tuttavia, è 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.

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

  Nota: *solo i componenti del server e-mail disponibili nell'elenco possono essere gestiti in remoto.*

- ***AVG 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:

- ***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 che vengono inviati, ricevuti o che circolano internamente tramite il ruolo HUB di MS Exchange.

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

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

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

  Disponibile esclusivamente per MS Exchange 2007, può essere installato sia per ruoli EDGE che HUB.

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

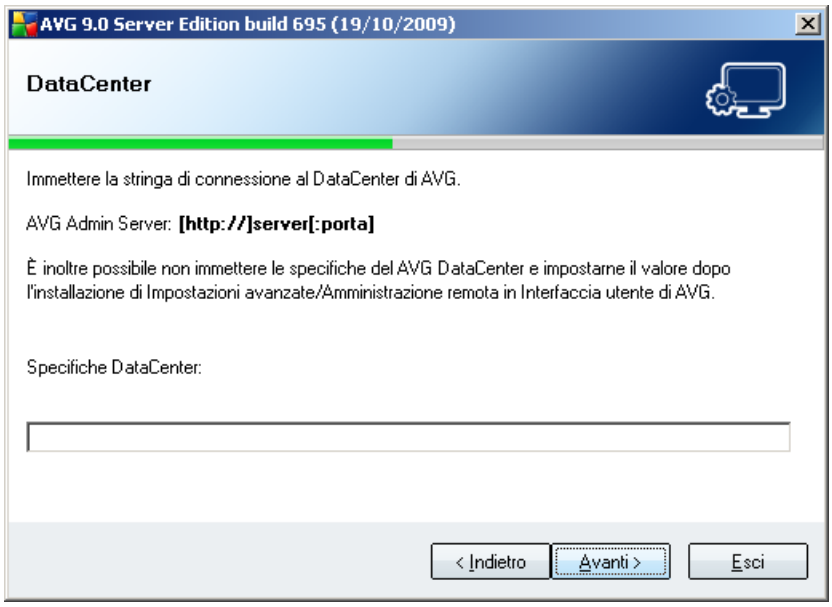
  Controlla tutti i messaggi e-mail archiviati nelle cassette postali degli utenti. Se vengono rilevati virus, questi vengono spostati in quarantena o completamente rimossi.

Nota: *sono disponibili diverse opzioni per MS Exchange 2007 e MS Exchange 2003.*

Continuare selezionando il pulsante ***Avanti***.

3.8. Installazione personalizzata - DataCenter

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



3.9. Riepilogo installazione

La finestra di dialogo ***Riepilogo installazione*** fornisce una panoramica di tutti i parametri del processo di installazione. Assicurarsi che tutte le informazioni siano corrette. In caso affermativo, fare clic sul pulsante ***Fine*** per continuare. Altrimenti, è possibile utilizzare il pulsante ***Indietro*** per tornare alla rispettiva finestra di dialogo e correggere le informazioni.

3.10. Installazione

Nella finestra di dialogo ***Installazione viene visualizzato l'avanzamento del processo di installazione. Non è necessario alcun intervento dell'utente.*** Al termine del completamento dell'installazione, verrà visualizzata la finestra di dialogo ***Installazione completata***.

3.11. Installazione completata

La finestra di dialogo ***Installazione completata*** è l'ultimo passaggio del processo di installazione di AVG. Adesso AVG è 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:

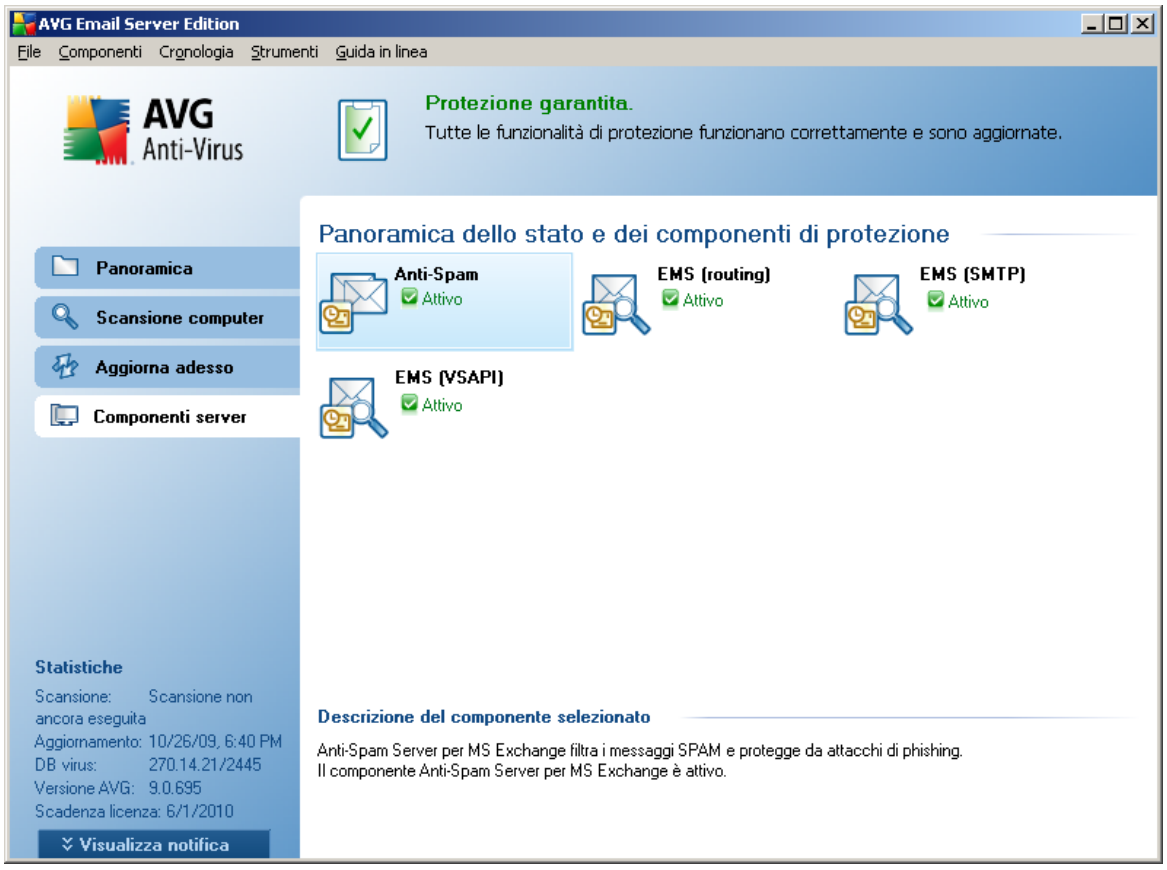
- ***Scansione e-mail per MS Exchange Server 2007***

- ***Scansione e-mail per MS Exchange Server 2000/2003***
- ***AVG per Kerio MailServer***

4. Scansione e-mail per MS Exchange Server 2007

4.1. Panoramica

Le opzioni di configurazione di AVG per MS Exchange Server 2007 sono completamente integrate in AVG 9.0 Email Server Edition come componenti server.



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 che vengono inviati, ricevuti o che circolano internamente tramite il ruolo HUB di MS Exchange.

  Disponibile per MS Exchange 2007, 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 in arrivo tramite l'interfaccia MS Exchange SMTP.

  Disponibile esclusivamente per MS Exchange 2007, può essere installato sia per ruoli EDGE che HUB.

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

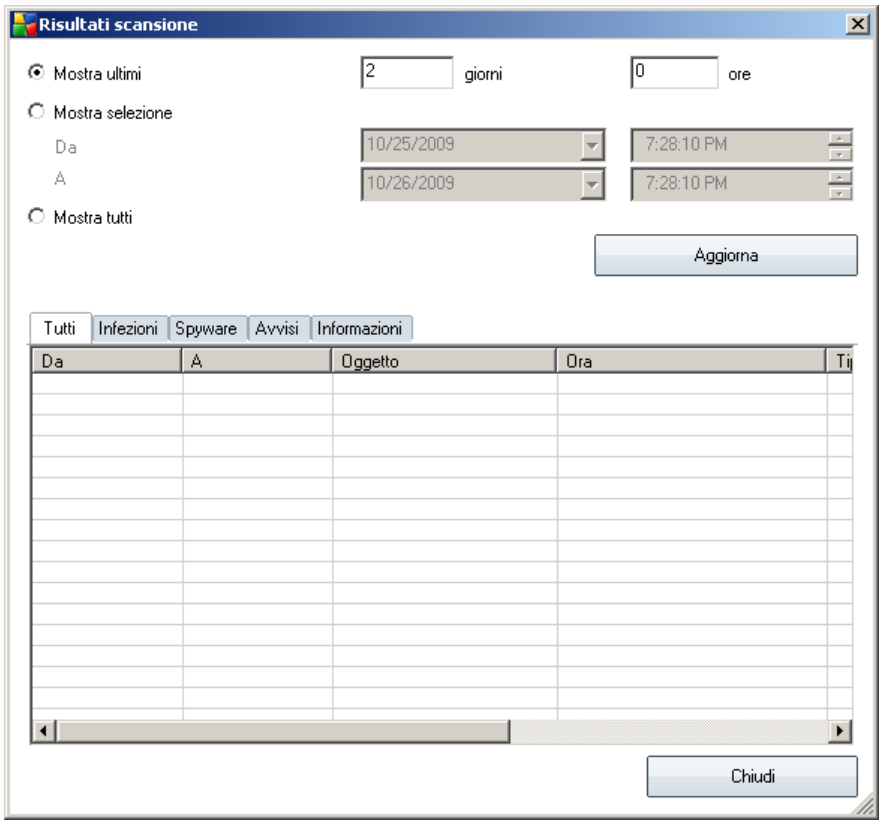
  Controlla tutti i messaggi e-mail archiviati nelle cassette postali degli utenti. Se vengono rilevati virus, questi vengono spostati in quarantena o completamente rimossi.

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:

Collegamenti disponibili:

- ***Risultati scansione***

  Apre 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.

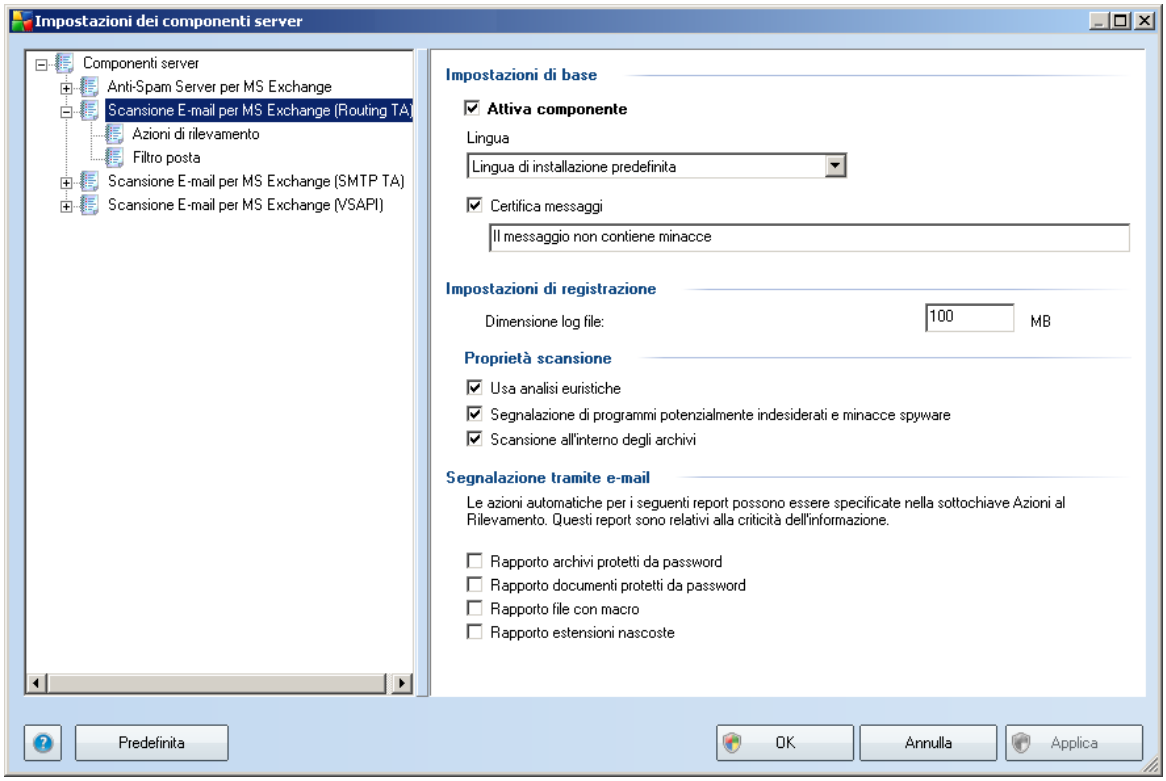
- ***Indietro***: selezionare questo pulsante per tornare alla panoramica dei componenti server.

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 per disattivare l'intero componente.
- ***Lingua*** - selezionare la lingua del componente preferita.
- ***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 preferite del file log. Valore predefinito: 100 MB.

La sezione ***Proprietà scansione***:

- ***Usa analisi euristiche*** - selezionare la presente casella per abilitare il metodo analisi euristiche durante la scansione.

- ***Segnalazione di programmi potenzialmente indesiderati e minacce*** - selezionare questa opzione per segnalare la presenza di programmi e spyware potenzialmente indesiderati.

- ***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 con tale elemento 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).

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)***.

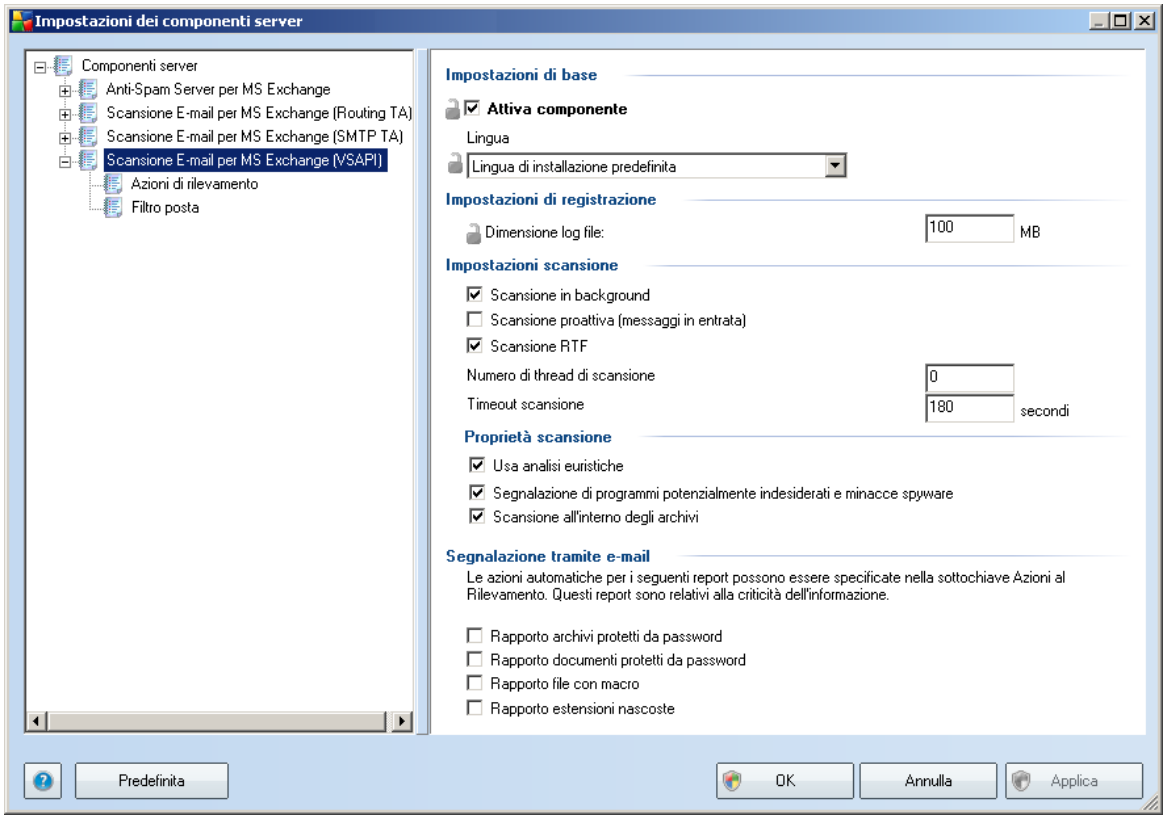
Sono inoltre disponibili le presenti sottovoci nella seguente struttura:

- ***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 per disattivare l'intero componente.
- ***Lingua*** - selezionare la lingua del componente preferita.

La sezione ***Impostazioni di registrazione***:

- ***Dimensione log file*** - selezionare le dimensioni preferite 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 dell'applicazione VSAPI 2.0/2.5. Fornisce la scansione in base ai thread dei database di messaggistica di Exchange. Ogni volta che viene rilevato un elemento che non è stato sottoposto a scansione con l'aggiornamento più recente del database dei virus all'interno delle cartelle della casella di posta dell'utente, esso viene inviato a AVG per MS Exchange 2007 per essere sottoposto a scansione. La scansione e la ricerca di oggetti non esaminati vengono eseguite in parallelo.

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

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

  È possibile abilitare o disabilitare la scansione proattiva VSAPI di 2.0/2.5 da 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 a bassa priorità (massimo 30 elementi). Questi vengono sottoposti a scansione in base al metodo FIFO (primo entrato, primo uscito). Se si accede ad un elemento che si trova in tale coda, esso assume elevata priorità.

  Nota: *i messaggi di overflow continueranno ad 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 il doppio del 'numero dei processori' più uno.

  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 analisi euristiche durante la scansione.
- ***Segnalazione di programmi potenzialmente indesiderati e minacce*** - selezionare questa opzione per segnalare la presenza di programmi e spyware potenzialmente indesiderati.
- ***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***

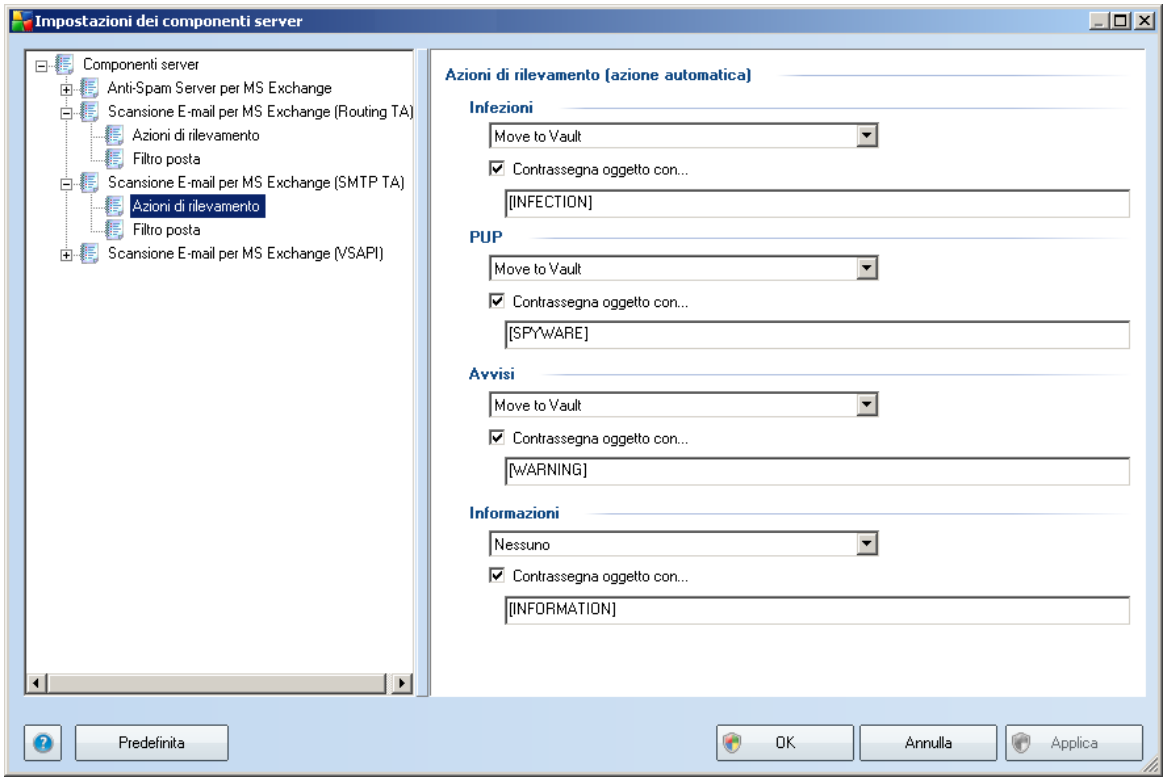
In genere, alcune di queste funzioni sono estensioni per l'utente dei servizi dell'interfaccia applicativa Microsoft VSAPI 2.0/2.5. Per informazioni dettagliate su VSAPI 2.0/2.5, vedere i seguenti collegamenti e i collegamenti accessibili tramite essi:

- 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. 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***

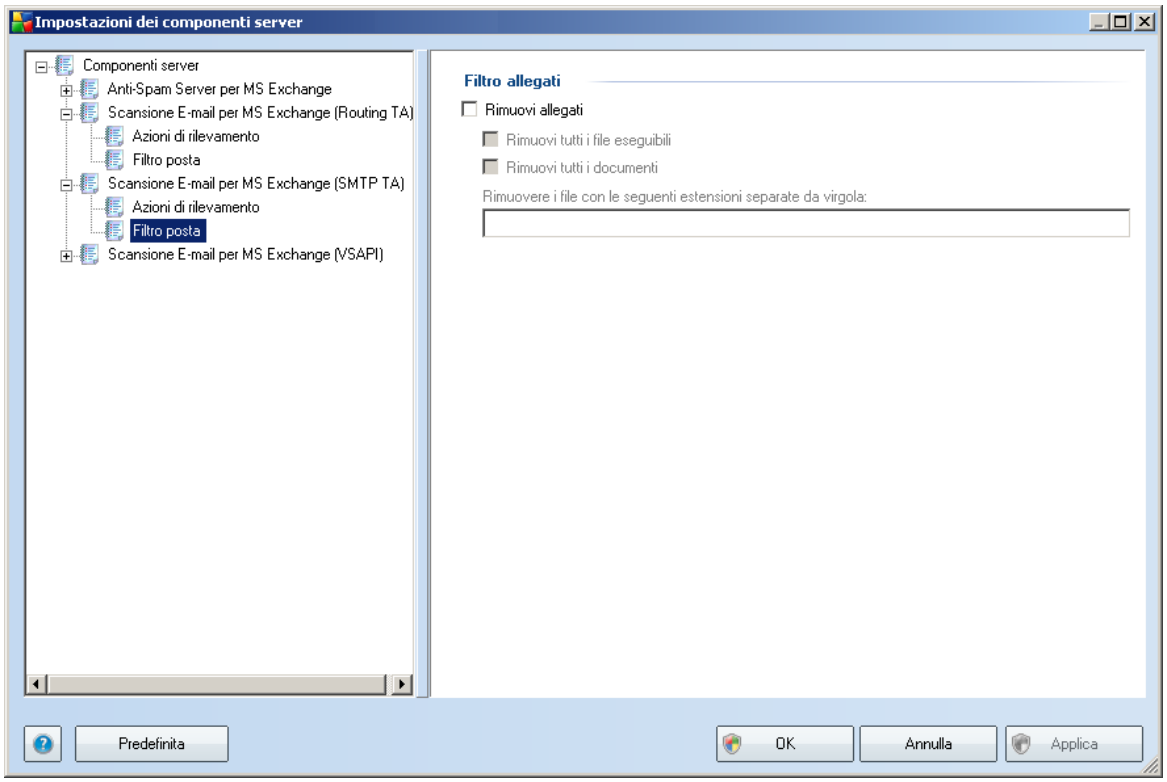
Utilizzare il menu a discesa per selezionare un'azione per ciascuna voce:

- ***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.*

4.6. 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 2000/2003

5.1. Panoramica

Le opzioni di configurazione di Scansione e-mail per MS Exchange Server 2000/2003 sono completamente integrate in AVG 9.0 Email Server Edition 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)***

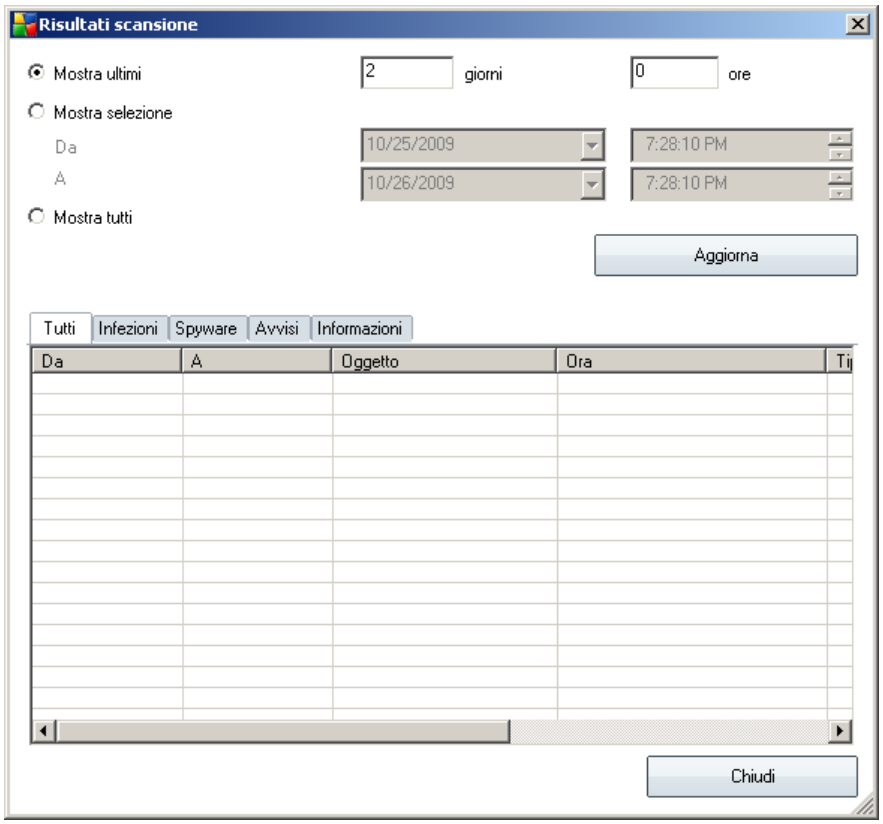
  Controlla tutti i messaggi e-mail archiviati nelle cassette postali degli utenti. Se vengono rilevati virus, questi vengono spostati in quarantena o completamente rimossi.

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:

Collegamenti disponibili:

- ***Risultati scansione***

  Apre 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.

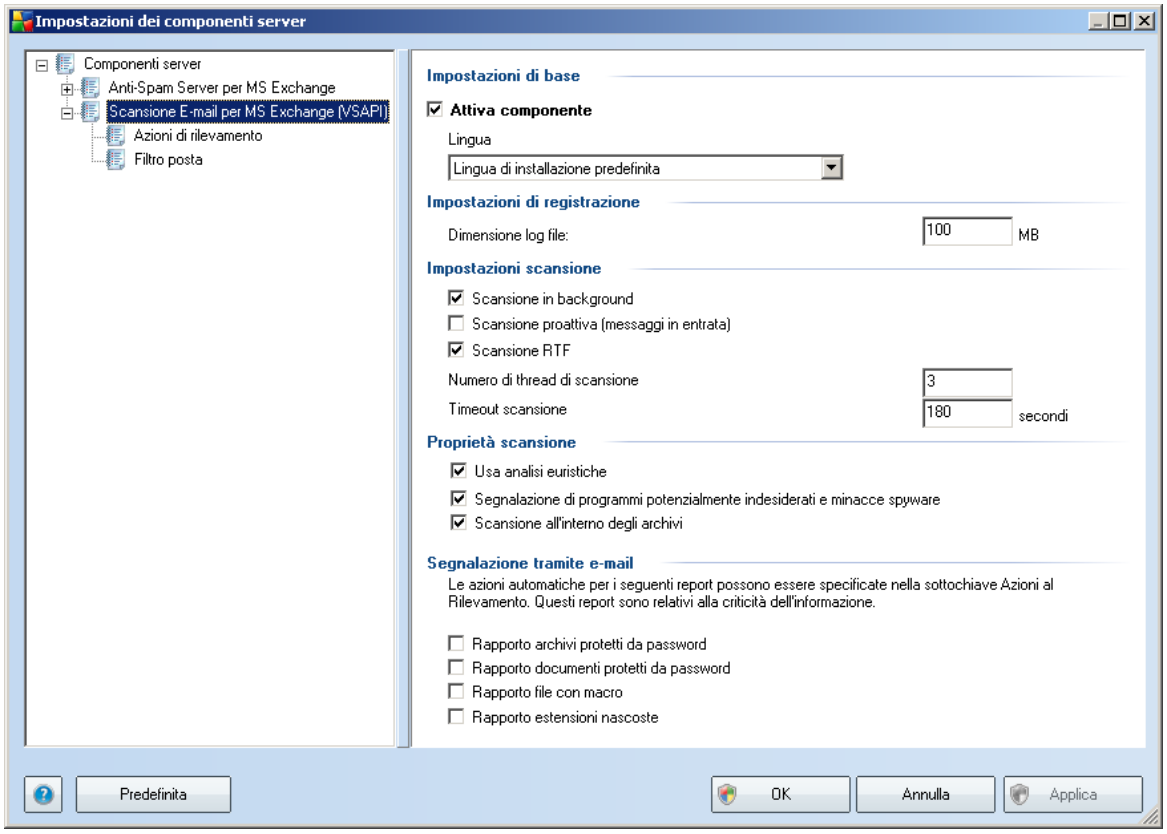
5.2. VSAPI 2.0

La scansione **API 2.0** (VSAPI 2.0 come indicato in MS Exchange 2000 Server) non consente l'eliminazione dei file infetti dei messaggi e-mail. Dato che non è possibile eliminare gli allegati infetti da virus dei messaggi e-mail, viene modificato il nome del file: AVG per Exchange 2000/2003 Server aggiunge l'estensione .virusinfo.txt al nome del file originale. Al contenuto del file viene sovrascritto un messaggio relativo al virus noto. Se il virus viene trovato direttamente nel messaggio, all'intero corpo del messaggio viene sovrascritta una nota che informa del rilevamento del virus nel messaggio.

La scansione **API 2.5** *(VSAPI 2.5 come indicato in MS Exchange 2003 Server)*consente anche l'eliminazione dei messaggi infetti. Questa funzionalità può essere configurata nella finestra di dialogo per la configurazione di AVG per MS Exchange 2000/2003 Server.

5.3. 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 per disattivare l'intero componente.
- ***Lingua*** - selezionare la lingua del componente preferita.

La sezione ***Impostazioni di registrazione***:

- ***Dimensione log file*** - selezionare le dimensioni preferite 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 dell'applicazione VSAPI 2.0/2.5. Fornisce la scansione in base ai thread dei database di messaggistica di Exchange. Ogni volta che viene rilevato un elemento che non è stato sottoposto a scansione con l'aggiornamento più recente del database dei virus all'interno delle cartelle della casella di posta dell'utente, esso viene inviato a AVG per MS Exchange 2007 per essere sottoposto a scansione. La scansione e la ricerca di oggetti non esaminati vengono eseguite in parallelo.

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

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

  È possibile abilitare o disabilitare la scansione proattiva VSAPI di 2.0/2.5 da 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 a bassa priorità (massimo 30 elementi). Questi vengono sottoposti a scansione in base al metodo FIFO (primo entrato, primo uscito). Se si accede ad un elemento che si trova in tale coda, esso assume elevata priorità.

  Nota: *i messaggi di overflow continueranno ad 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 il doppio del 'numero dei processori' più uno.

  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 analisi euristiche durante la scansione.
- ***Segnalazione di programmi potenzialmente indesiderati e minacce*** - selezionare questa opzione per segnalare la presenza di programmi e spyware potenzialmente indesiderati.
- ***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:80/support/kb/articles/Q285/6/67.ASP per informazioni generali su VSAPI 2.0 in Exchange 2000 Server Service Pack 1
- http://support.microsoft.com/default.aspx?scid=kb;en-us;328841&Product=exch2k per informazioni sull'interazione tra il software

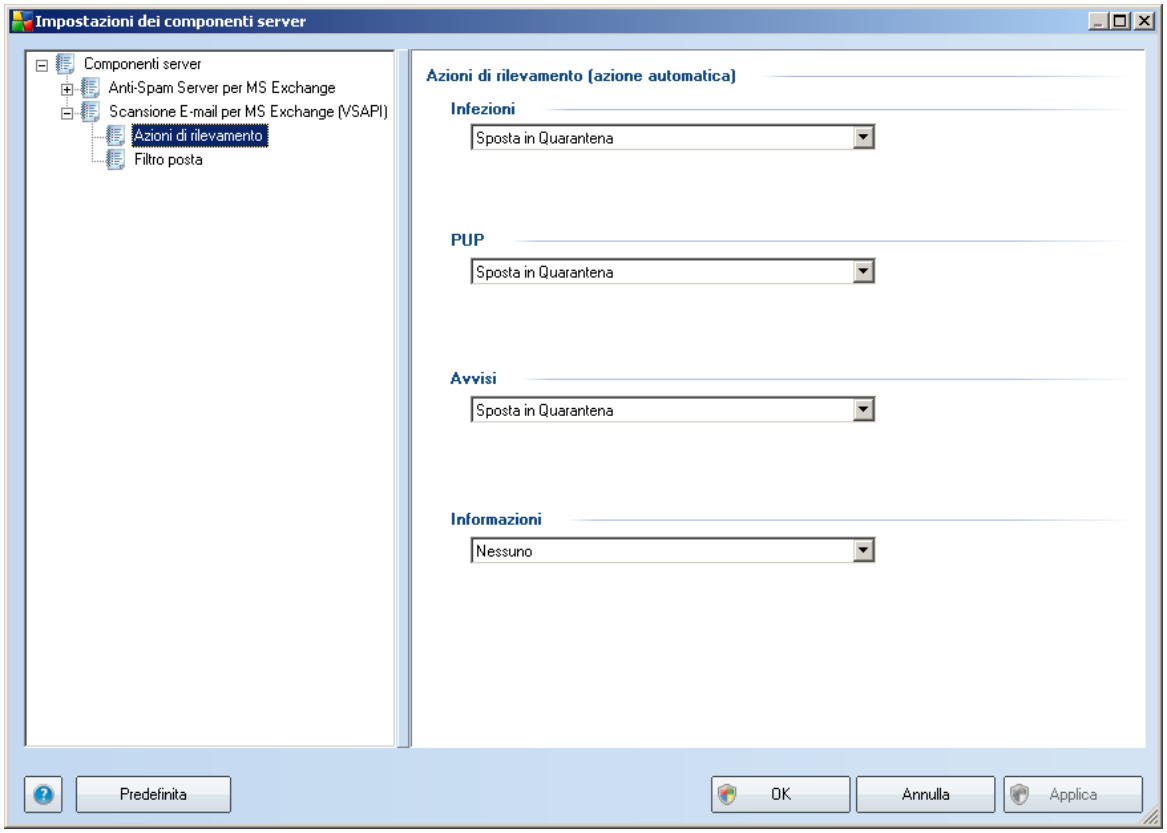
antivirus e Exchange

- 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***

5.4. Azioni_di_rilevamento



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

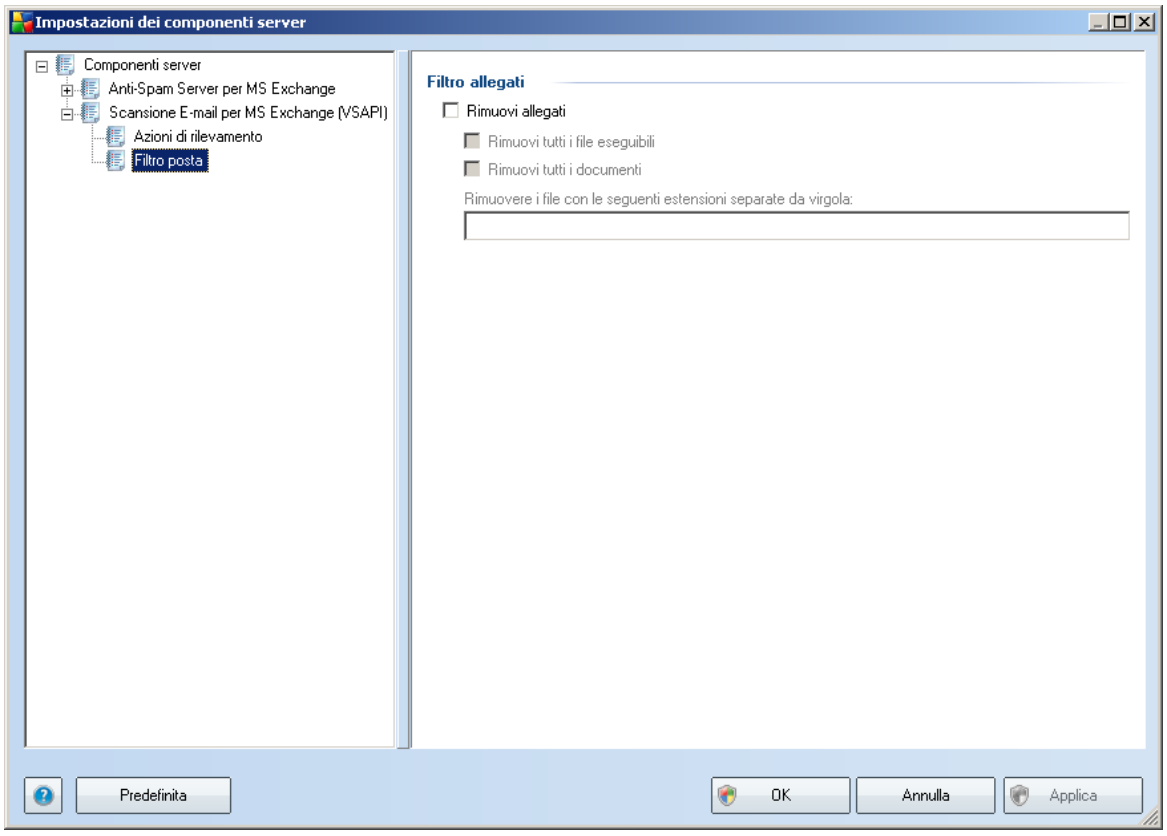
Tali azioni sono disponibili per le seguenti voci:

- ***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.

5.5. Filtro posta



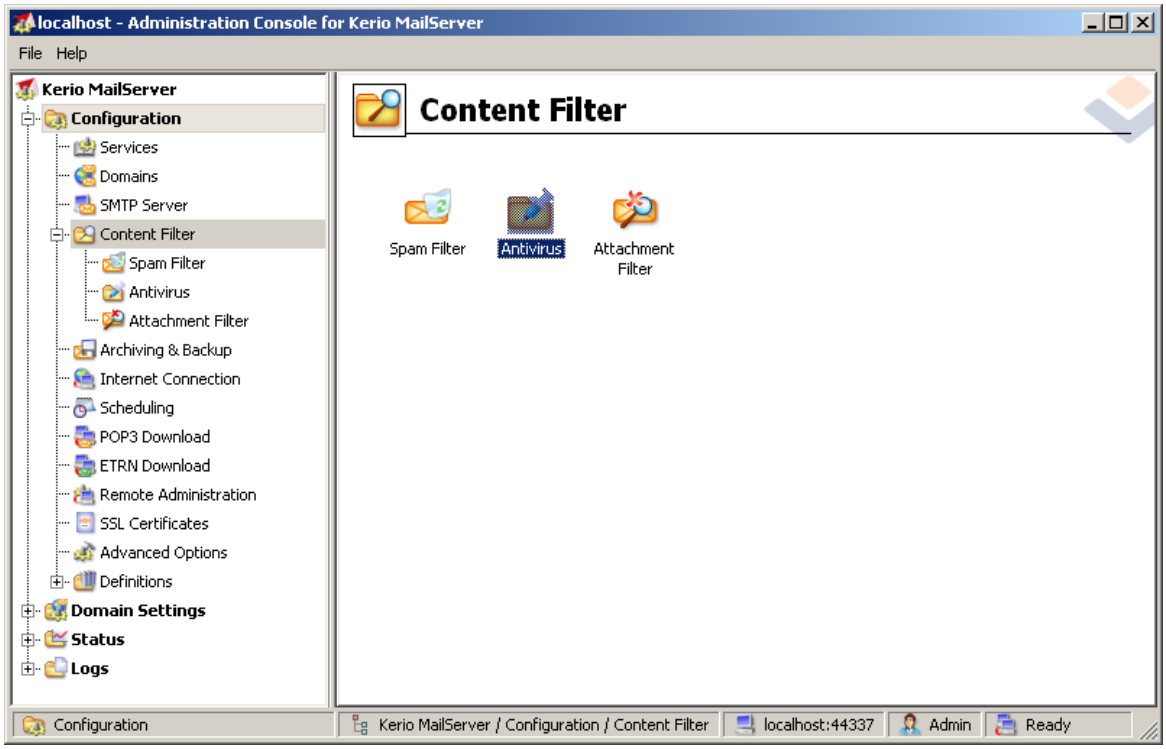
Nella sottovoce ***Filtro posta*** è possibile selezionare gli eventuali allegati da rimuovere automaticamente. Sono disponibili le seguenti opzioni:

- ***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:

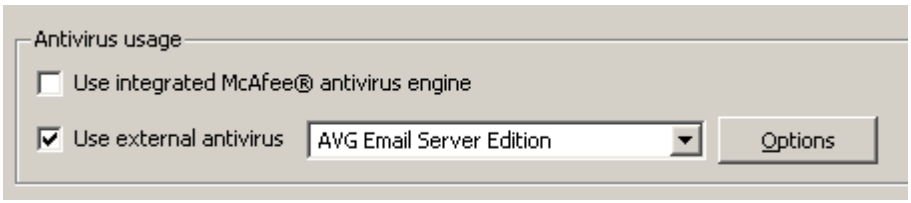


Se si fa clic su Filtro contenuti viene visualizzata la finestra di dialogo con i tre elementi:

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

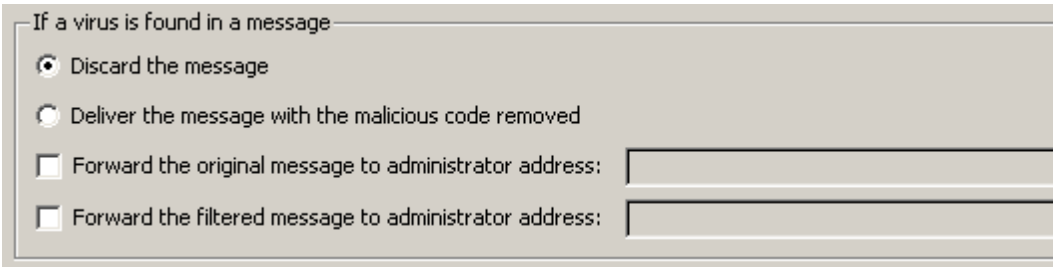
6.1.1. Antivirus

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:

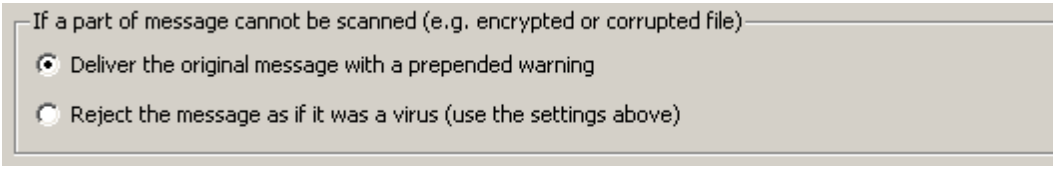
- ***Se viene rilevato un virus in un messaggio***



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)***



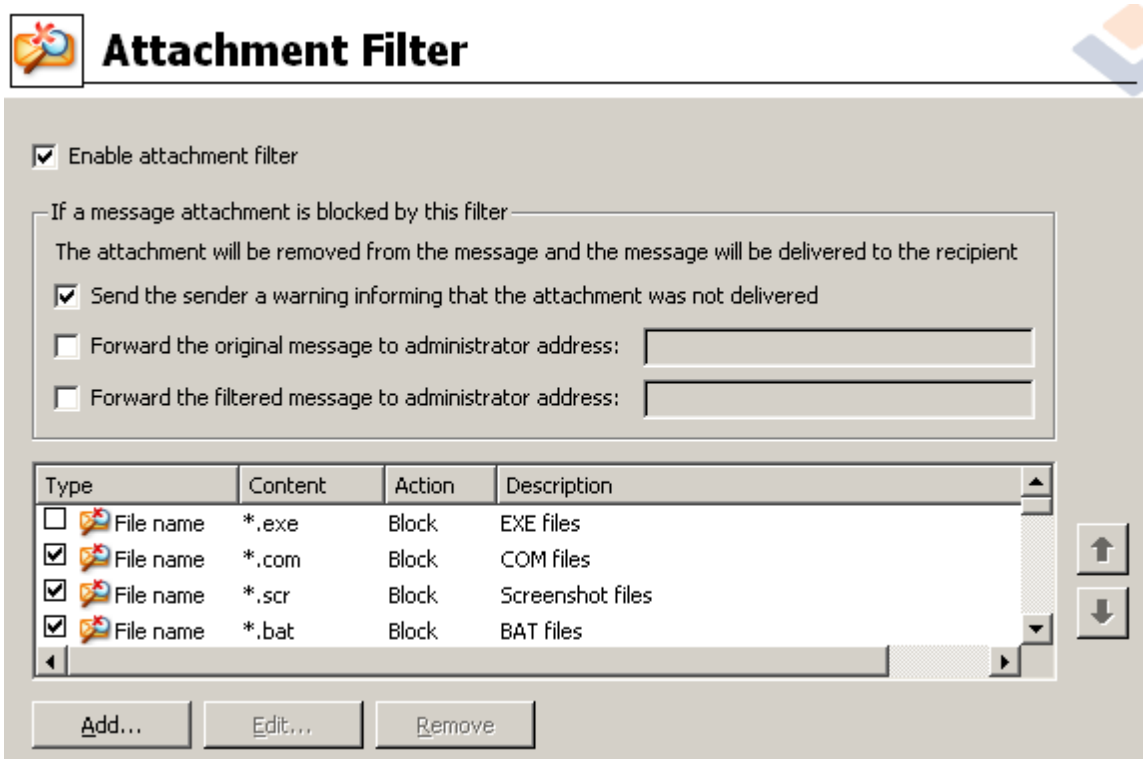
Questo frame consente di specificare l'azione da eseguire se non è possibile esaminare una parte del messaggio o dell'allegato:

  - ***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 di posta 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 inviato***

  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 data nel campo Contenuto. 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 (consente di accettare l'allegato) e Blocca (consente di bloccare l'allegato come definito nella finestra di dialogo della scheda Azione).
- ***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:

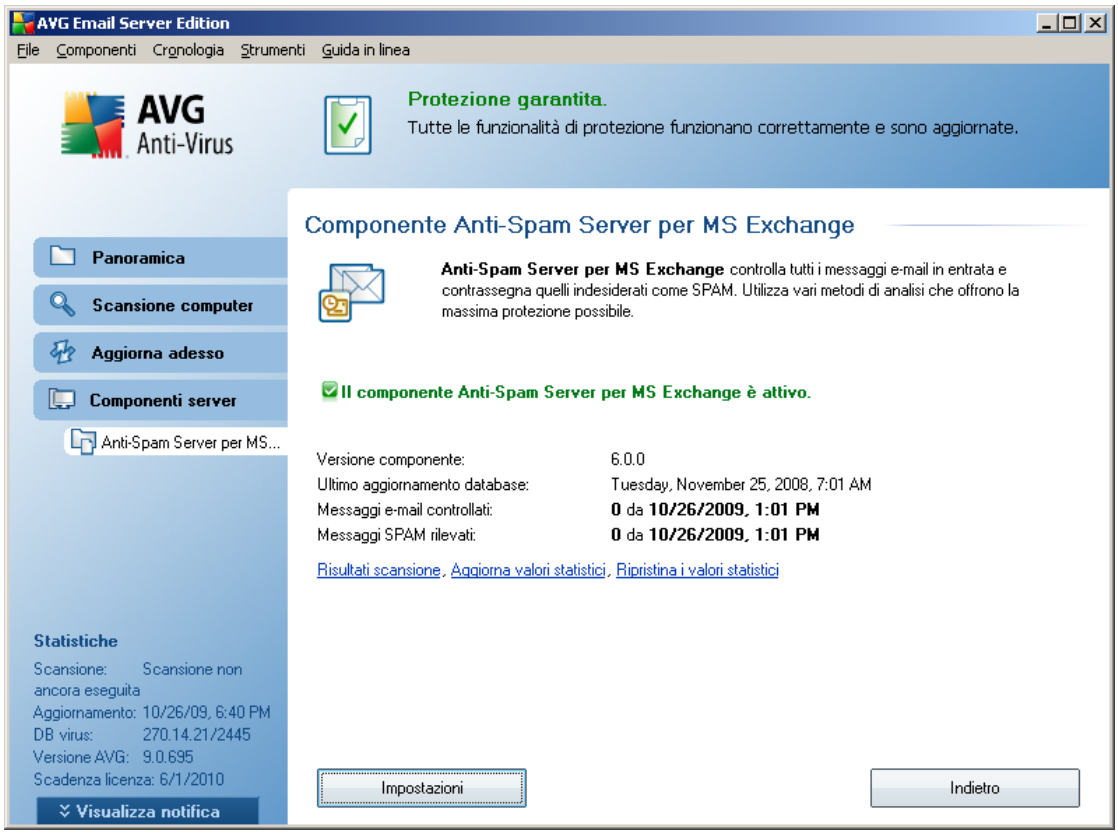
- Nel campo Descrizione è possibile scrivere una breve descrizione dell'allegato da filtrare.

- 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 Anti-Spam

7.1. Interfaccia Anti-Spam

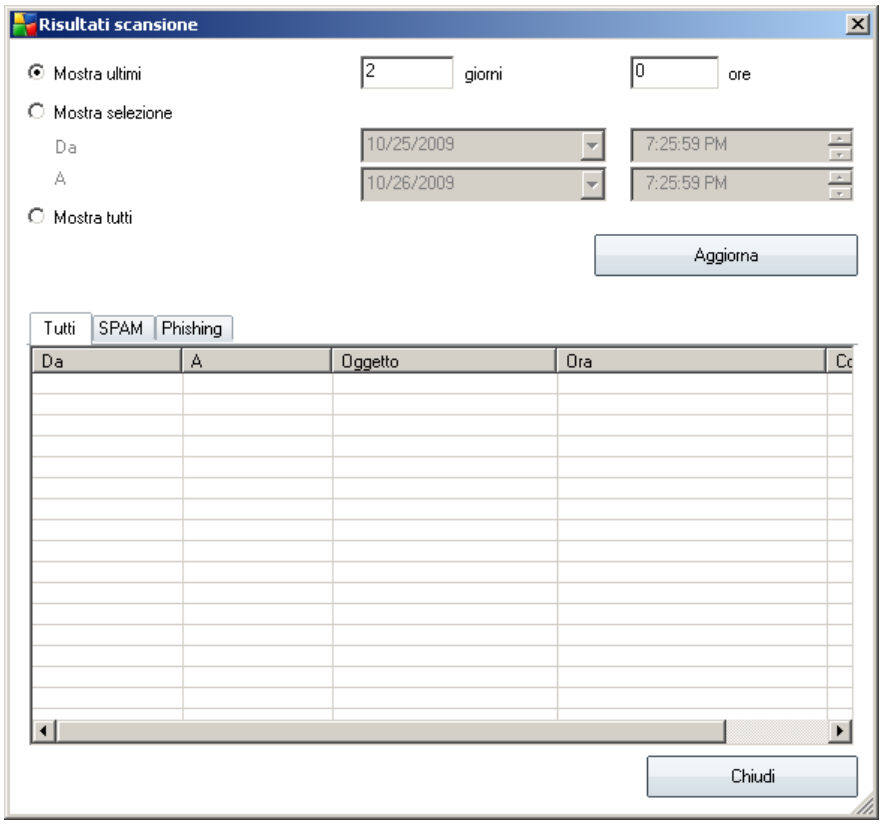


La finestra di dialogo del componente server ***Anti-Spam*** è disponibile nella sezione ***Componenti server*** (menu a sinistra). Contiene brevi informazioni sulla funzionalità del componente server, informazioni sul relativo stato corrente (ad esempio *Il componente Anti-Spam Server per MS Exchange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

Collegamenti disponibili:

- ***Risultati scansione***

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



Qui è possibile controllare i messaggi rilevati come SPAM (messaggi indesiderati) o attacco di phishing (tentativo di sottrarre dati personali, dati bancari, informazioni sull'identità e così via). 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:

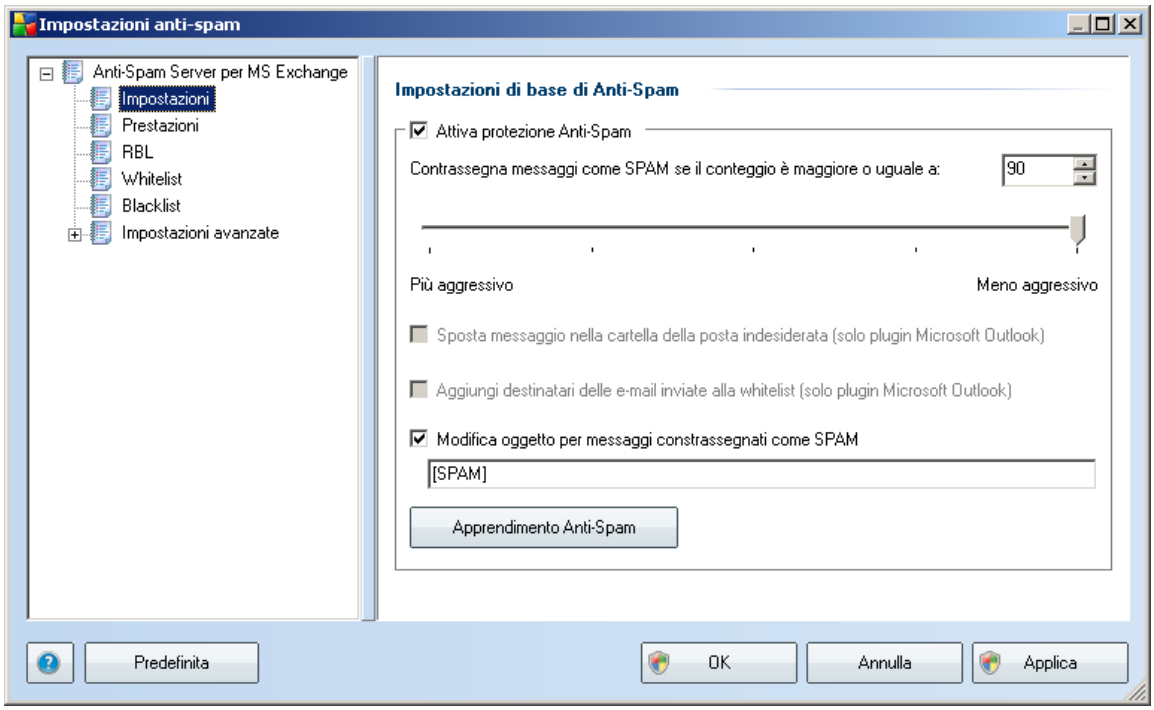
- ***Impostazioni***: selezionare questo pulsante per aprire Impostazioni Anti-Spam.
- ***Indietro***: selezionare questo pulsante per tornare alla panoramica dei componenti server.

7.2. Principi Anti-Spam

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

Anti-Spam controlla tutti i messaggi di posta elettronica 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 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 a SPAM*) in base a diverse tecniche di scansione dinamica. È possibile regolare l'impostazione ***Contrassegna messaggi come spam se il conteggio è maggiore o uguale a*** digitando il valore (*da 0 a 100*) oppure spostando il dispositivo di scorrimento verso sinistra o verso destra (*utilizzando il dispositivo di scorrimento, l'intervallo di valori è compreso tra 50 e 90*).

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

- ***Valore compreso tra 90 e 99***: 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 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 tra 1 e 59***: configurazione particolarmente aggressiva. È probabile che insieme ai messaggi e-mail contenenti spamvengano filtrati anche i messaggi normali. Questo intervallo di valori non è consigliato.

- ***Valore 0***: in questa modalità, si riceveranno solo i messaggi e-mail provenienti dai mittenti inclusi nella ***whitelist***. Gli altri messaggi e-mail verranno considerati spam. ***Questo intervallo di valori non è consigliato.***

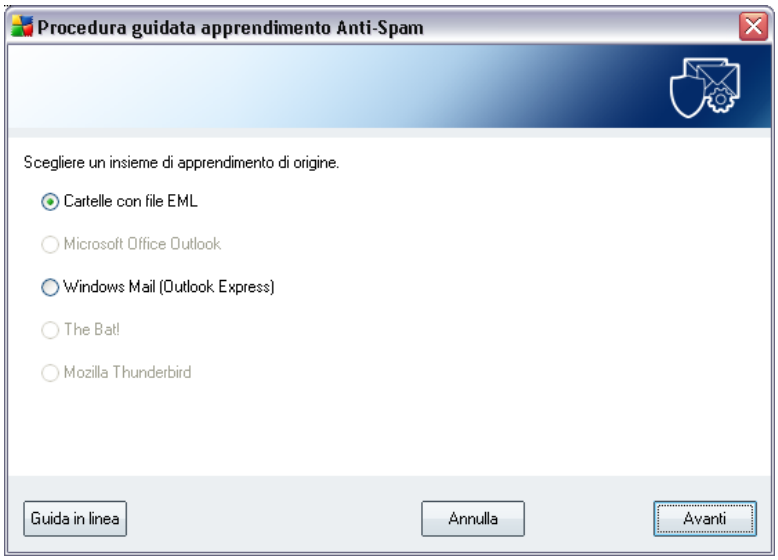
È possibile definire ulteriormente il modo in cui trattare i messaggi e-mail spam rilevati:

- ***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.

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

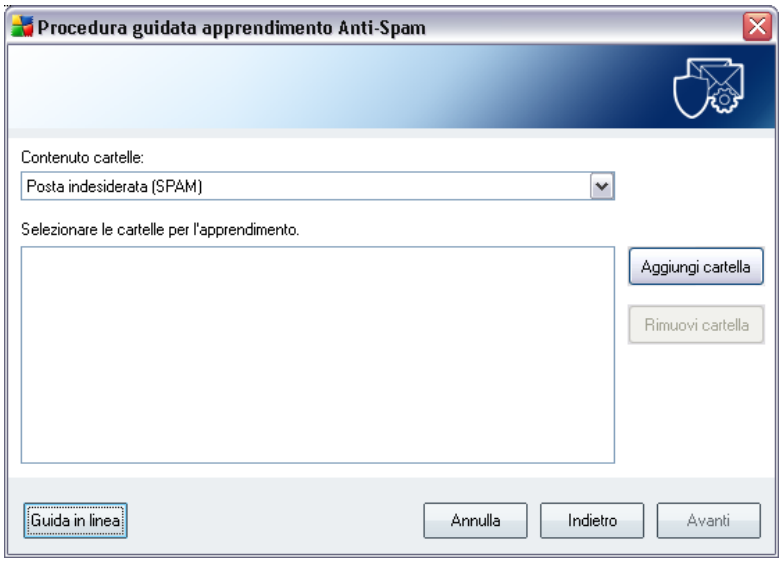
Per un processo di apprendimento più semplice e rapido, è innanzitutto consigliabile ordinare i messaggi e-mail nelle cartelle, in modo che la cartella utilizzata per l'apprendimento contenga solo i messaggi per l'apprendimento (desiderati o indesiderati). Questa operazione non è tuttavia indispensabile, 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 a questo passaggio dipende dalla selezione precedente.

Cartelle con file EML



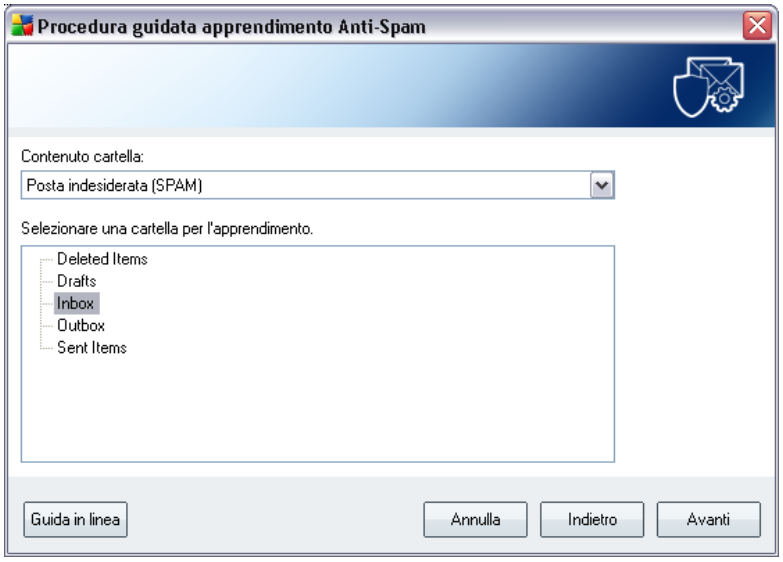
In questa finestra di dialogo selezionare la cartella contenente i messaggi che si desidera utilizzare per l'apprendimento. Fare clic sul pulsante ***Aggiungi cartella*** per individuare la cartella con i file .eml (*messaggi e-mail salvati*). La cartella selezionata verrà visualizzata nella finestra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

E-mail client specifico

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

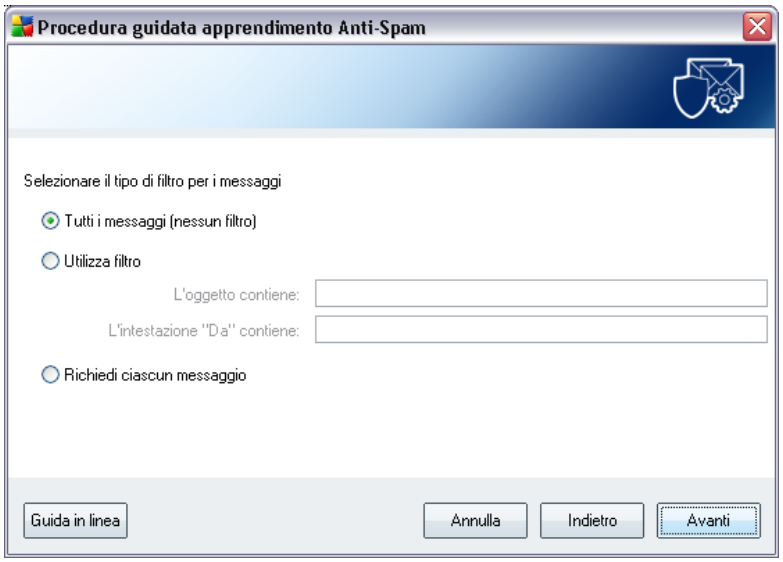


Nota: *se si utilizza Microsoft Office Outlook, verrà richiesto di selezionare il primo profilo di MS Office Outlook.*

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)***.

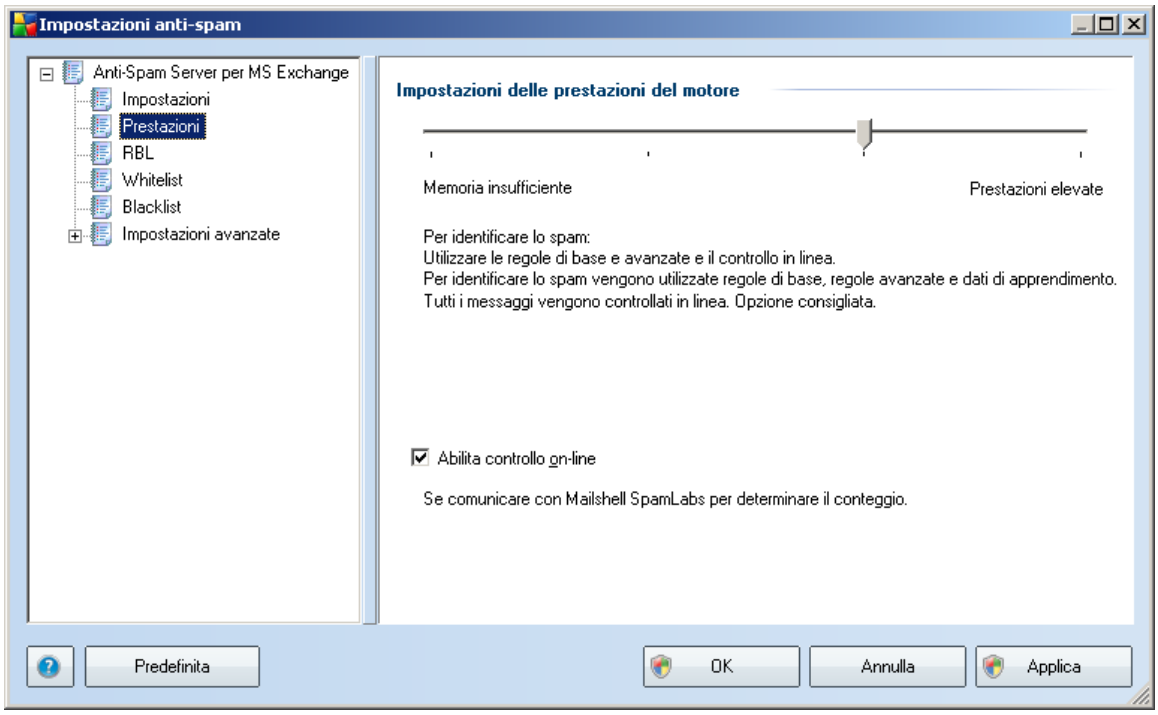
Se si hanno dubbi sui messaggi contenuti nella cartella e si desidera che durante la procedura guidata venga richiesta una conferma per ogni singolo messaggio (al fine di determinare se utilizzarlo o meno per l'apprendimento), selezionare l'opzione ***Chiedi per ogni messaggio***.

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*** *del menu di esplorazione visualizzato a sinistra*) offre le impostazioni delle prestazioni del componente ***Anti-Spam***. Spostare il dispositivo di scorrimento a destra o a sinistra per modificare il livello di 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 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.

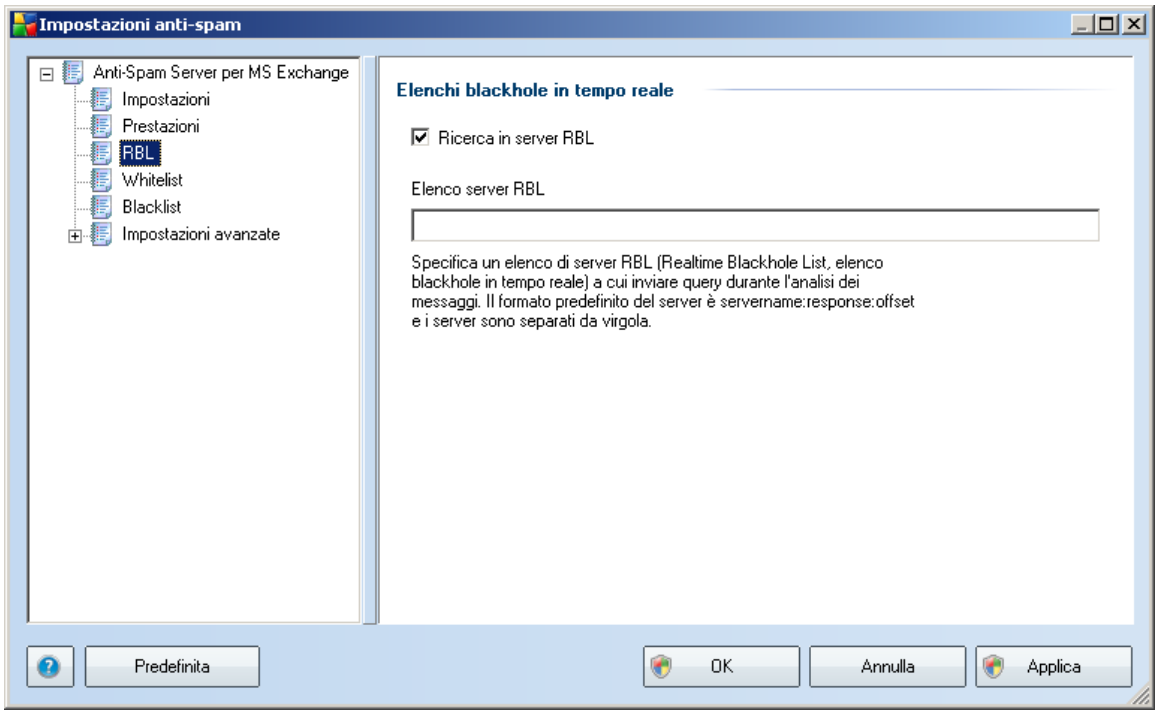
La voce ***Abilita controllo on-line*** è attiva per impostazione predefinita. Ne risulta un rilevamento dello spam più preciso tramite la comunicazione con i server Mailshell, ovvero i dati sottoposti a scansione verranno confrontati con i database Mailshell on-

line.

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 modificabile denominata ***Elenchi blackhole in tempo reale (RBL)***:



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

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

I database dei server RBL contengono le impronte digitali di spam più aggiornate, per

fornire il rilevamento di spam migliore e più accurato. La funzione è particolarmente utile per gli utenti che ricevono grandi quantità di messaggi di spam normalmente non rilevati dal motore Anti-Spam.

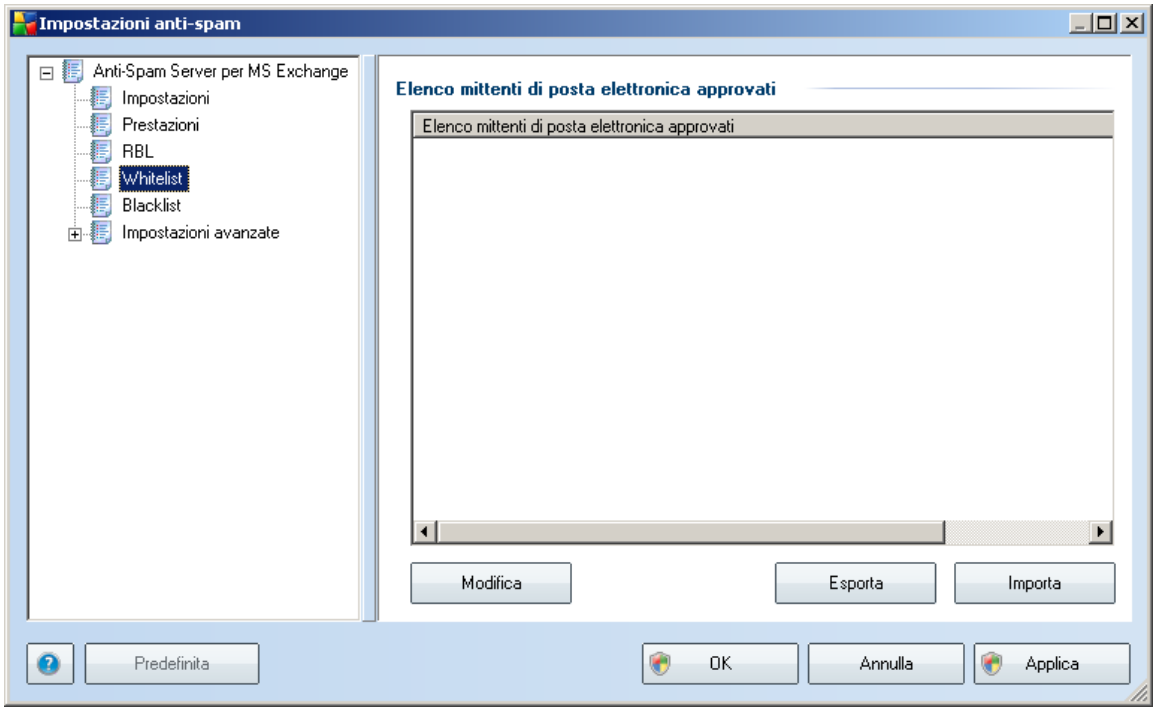
La funzione ***Elenco server RBL*** consente di definire le posizioni dei server RBL specifici. Per impostazione predefinita, sono specificati due indirizzi server RBL. Se non si è un utente esperto e se non si necessita veramente di modificare queste impostazioni, si consiglia di mantenere le impostazioni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

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

Non vengono inviati dati personali sul 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 generanno 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 e-mail o importando tutto l'elenco di indirizzi. Sono disponibili i seguenti pulsanti di controllo:

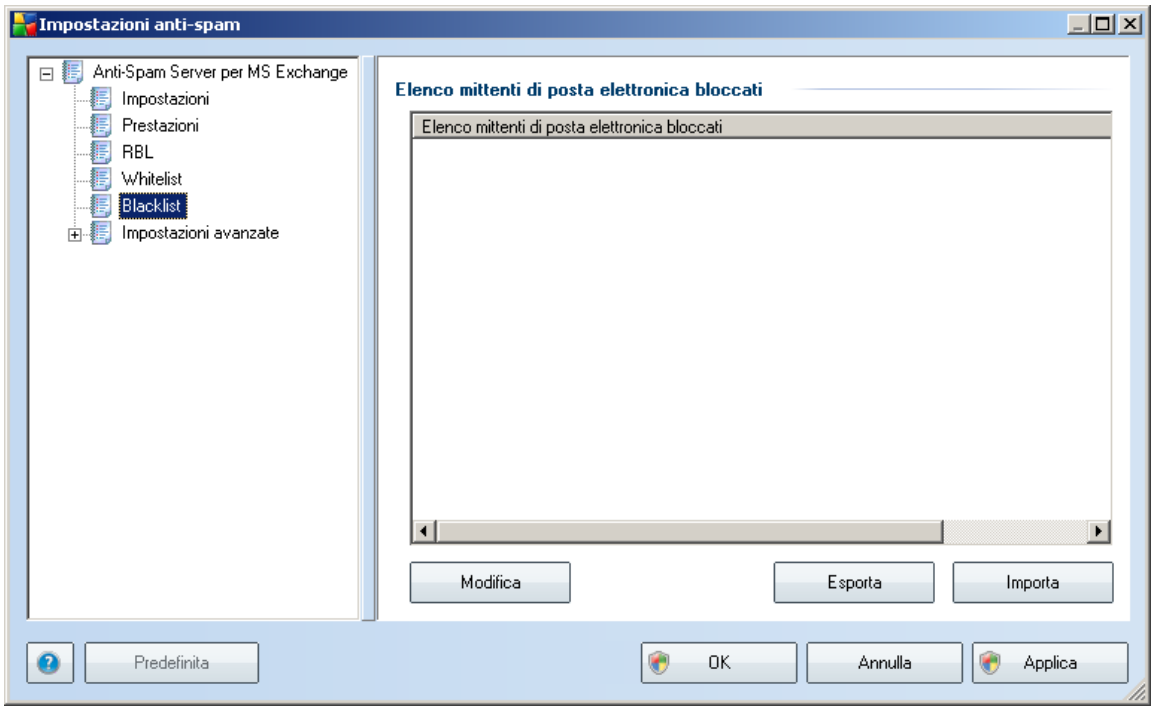
- ***Modifica****: selezionare questo pulsante per aprire una finestra di dialogo in cui è possibile immettere manualmente un elenco di indirizzi (è inoltre possibile utilizzare il metodo copia e incolla*). Immettere una voce (mittente o nome di dominio) per riga.

- ***Importa***: 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 di input deve presentare il formato testo normale e il contenuto deve includere una sola voce (indirizzo 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.

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 *aziendaspamming.com*), da cui si prevedono 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 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***: 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 di input deve presentare il formato testo normale e il contenuto deve includere una sola voce (indirizzo 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.

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:

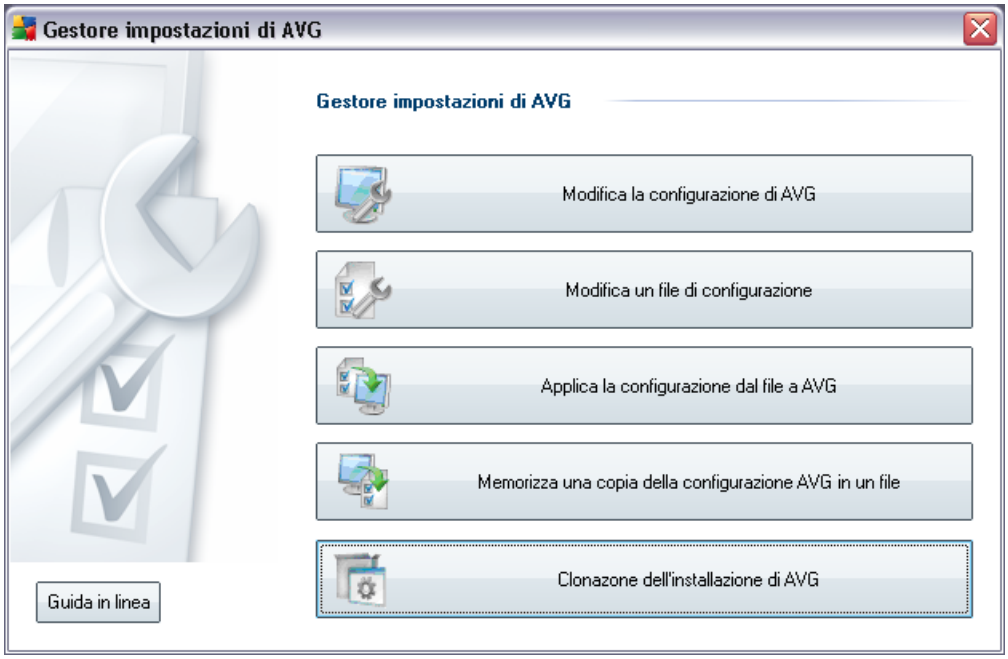
- ***Cache*** : impronte digitali, reputazione dominio, LegitRepute
- ***Apprendimento***: apprendimento di parole, cronologia conteggio, offset conteggio, numero massimo di parole, soglia di apprendimento automatico, peso, buffer scrittura
- ***Filtraggio***: elenco lingue, elenco paesi, IP approvati, 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 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 <%VER%>/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***

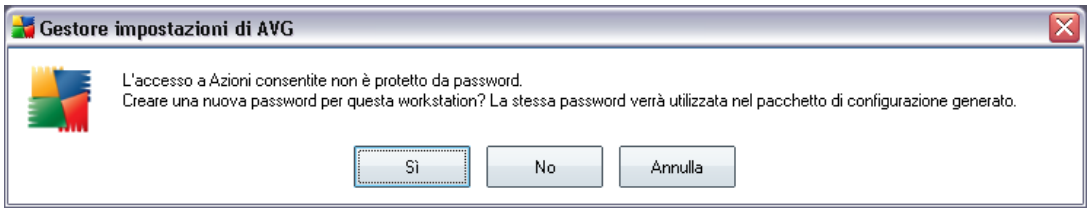
  Se si dispone già di un file di configurazione di AVG (.pck), utilizzare questo pulsante per aprire il file per la modifica. Dopo aver confermato le modifiche tramite il pulsante ***OK*** o ***Applica***, il file conterrà le nuove impostazioni.

- ***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***

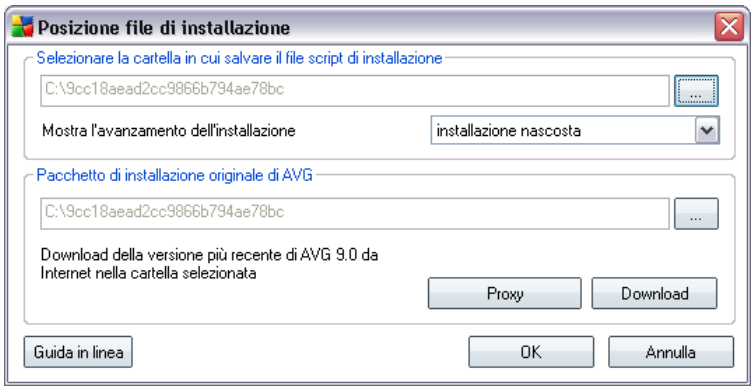
  Utilizzare questo pulsante per salvare il file di configurazione di AVG (.pck) dell'installazione locale di AVG. Se non è stata impostata una password per le azioni consentite, potrebbe venire visualizzata la seguente finestra di dialogo:



  Rispondere ***Sì*** se si desidera impostare la password per accedere ora a Elementi consentiti, quindi completare le informazioni richieste e confermare la scelta. Rispondere ***No*** per ignorare la creazione della password e procedere con il salvataggio della configurazione 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 attenzione da parte dell'utente, ma il progresso sarà interamente 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 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 a breve. 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 sopra.

9. FAQ 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/it.

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***.