AVG Email Server Edition 2013

Manuale per l'utente

Revisione documento 2013.01 (20.11.2012)

Sommario

1. Introduzione

Questa guida per l'utente fornisce la documentazione completa relativa a **AVG Email Server Edition 2013**.

Complimenti per l'acquisto di AVG Email Server Edition 2013!

AVG Email Server Edition 2013 è un elemento della gamma di prodotti AVG pluripremiati progettata per offrire la tranquillità totale e la protezione completa del server. Analogamente a tutti i prodotti AVG, **AVG Email Server Edition 2013** 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 Email 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 2013 consente di proteggere i server email in esecuzione con 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 email:

- Versione MS Exchange 2003 Server
- Versione MS Exchange 2007 Server
- Versione MS Exchange 2010 Server
- Kerio MailServer 6.7.2 e versioni successive

2.3. Requisiti hardware

I requisiti hardware minimi per **AVG Email Server Edition 2013** 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 2013** 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 2013**. È necessario eseguire la disinstallazione della versione precedente manualmente, utilizzando la funzionalità standard di Windows.

- Dal menu ***Start/Impostazioni/Pannello di controllo/Installazione applicazioni*** selezionare il programma desiderato dall'elenco del software installato (in alternativa, è possibile utilizzare il menu

Start/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/en-us/download/details.aspx?id=9664

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

Service Pack per MS Exchange 2010 Server (opzionale):

http://www.microsoft.com/en-us/download/details.aspx?id=28190

3. Processo di installazione di AVG

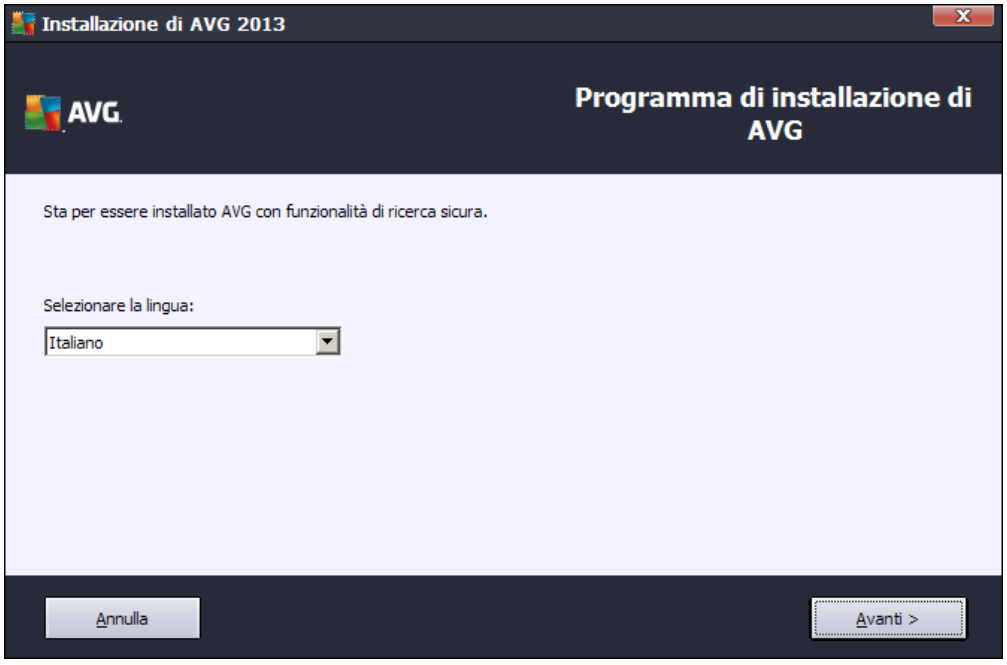
Per installare AVG nel computer è preferibile disporre del file di installazione più recente. È possibile utilizzare il file di installazione presente nel CD contenuto nella confezione del prodotto, tuttavia questo file potrebbe non essere aggiornato. Pertanto è consigliabile procurarsi il file di installazione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

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 License Number. Prima di avviare l'installazione, assicurarsi che sia disponibile. Il numero si trova sulla confezione del CD. Se la copia di AVG è stata acquistata via Web, il License Number viene fornito tramite email.

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:

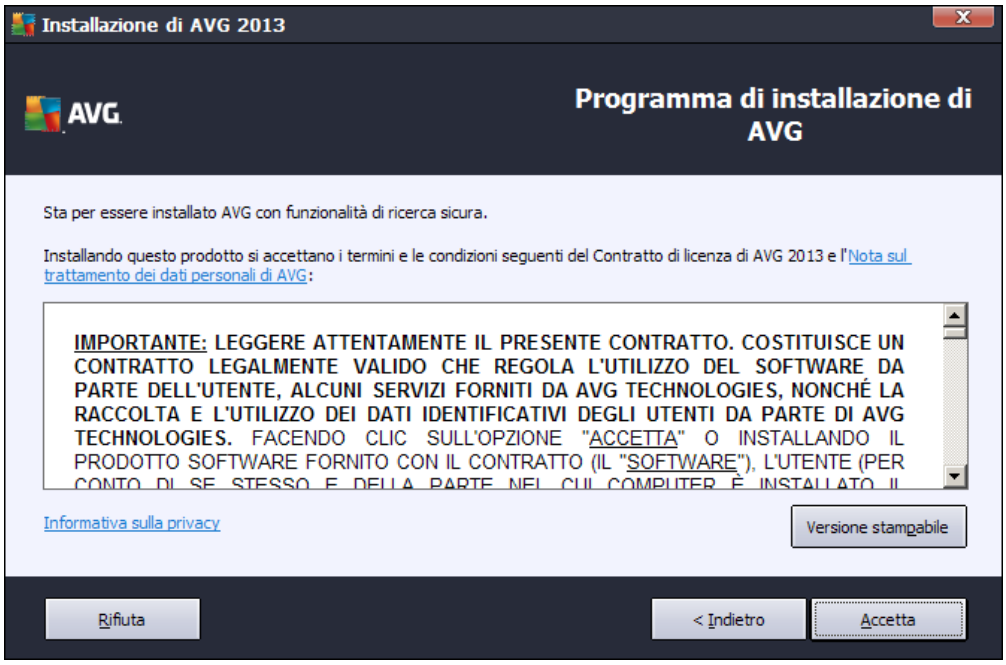
3.1. Avvio dell'installazione



La prima finestra del processo di installazione visualizzata è quella ***introduttiva***. Da qui è possibile selezionare la lingua utilizzata per il processo di installazione e fare clic sul pulsante ***Avanti***.

Sarà inoltre possibile scegliere ulteriori lingue per l'interfaccia dell'applicazione in un secondo momento durante il processo di installazione.

3.2. Contratto di licenza

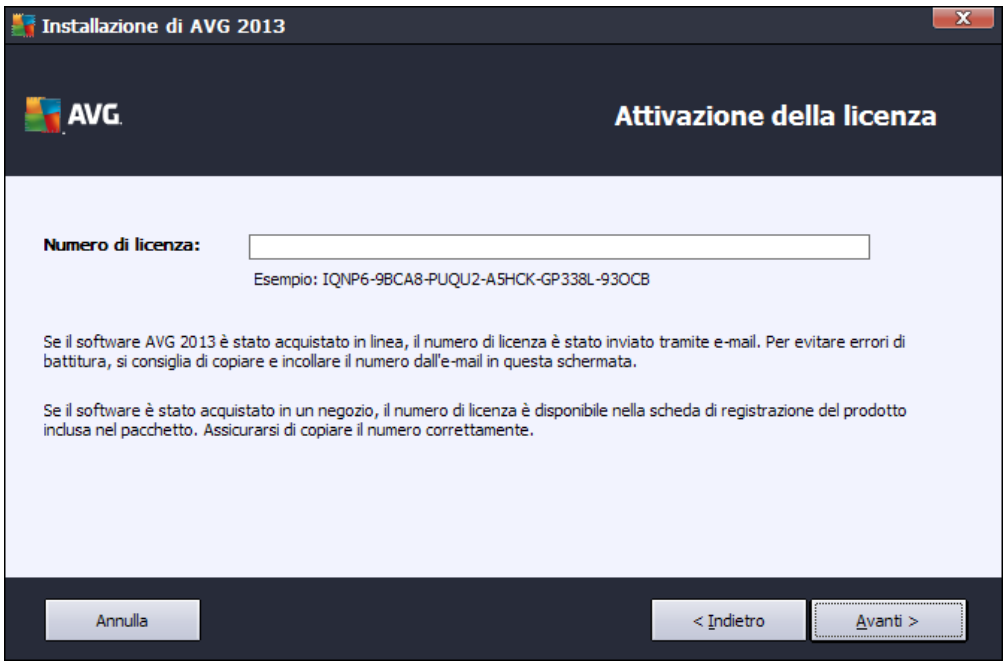


Questa finestra di dialogo consente di leggere le condizioni di licenza. Utilizzare il pulsante ***Versione stampabile*** per aprire il testo della licenza in una nuova finestra. Selezionare il pulsante ***Accetta*** per confermare e procedere alla finestra di dialogo successiva.

3.3. Attivazione della licenza

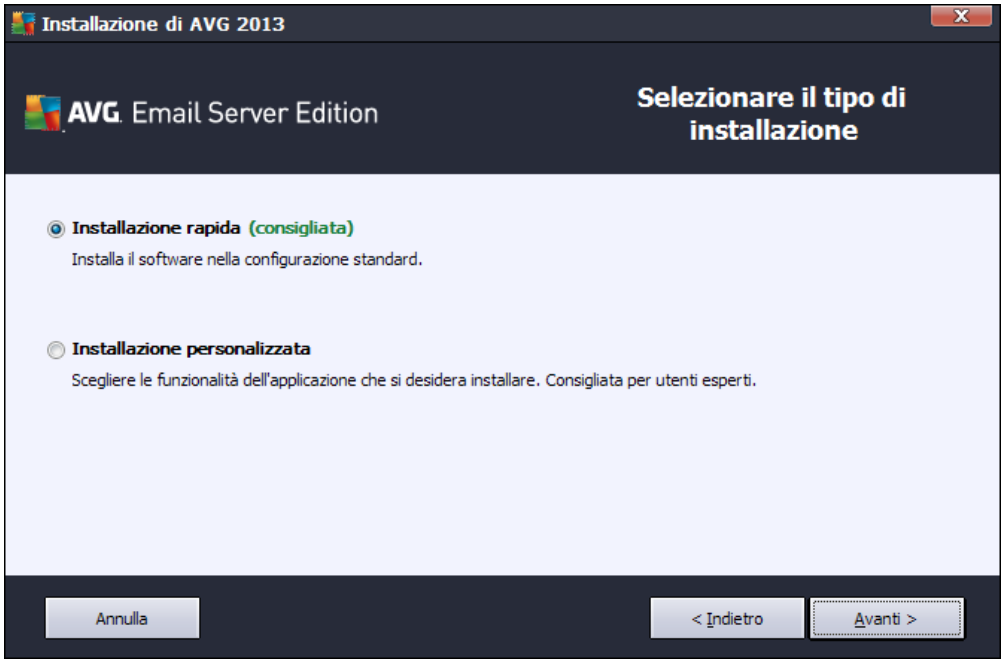
Nella finestra di dialogo ***Attivazione della licenza*** è necessario immettere il License Number.

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



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

3.4. Selezionare il tipo di installazione



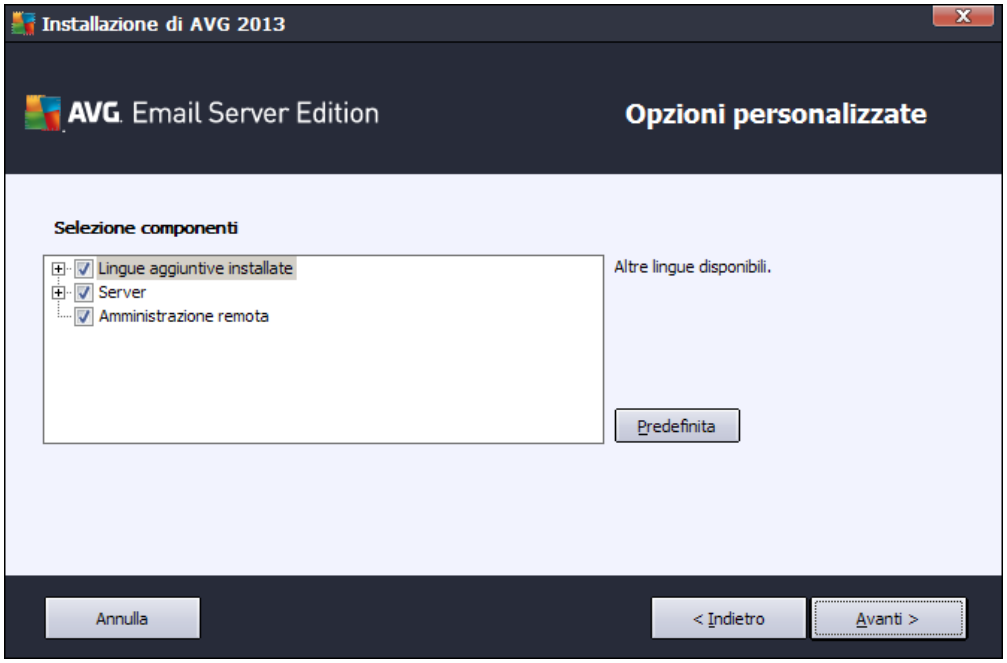
La finestra di dialogo ***Selezionare il tipo di installazione*** offre due opzioni di installazione: ***Installazione rapida*** e ***Installazione personalizzata***.

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

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.

Dopo aver selezionato Installazione personalizzata, nella parte inferiore della finestra di dialogo verrà visualizzata la sezione ***Cartella di destinazione***. Consente di specificare il percorso in cui AVG deve essere installato. 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.

3.5. Installazione personalizzata - Opzioni personalizzate



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.

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

- ***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 (nel ramo ***Server***):

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

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

- ***Scansione Email per MS Exchange (routing Transport Agent)***

  Controlla tutti i messaggi email che vengono inviati, ricevuti o che circolano internamente tramite il ruolo HUB di MS Exchange.

- ***Scansione Email per MS Exchange (SMTP Transport Agent)***

  Controlla tutti i messaggi email ricevuti tramite l'interfaccia MS Exchange SMTP (è possibile eseguire l'installazione sia per ruoli EDGE che HUB).

- ***Scansione Email per MS Exchange (VSAPI)***

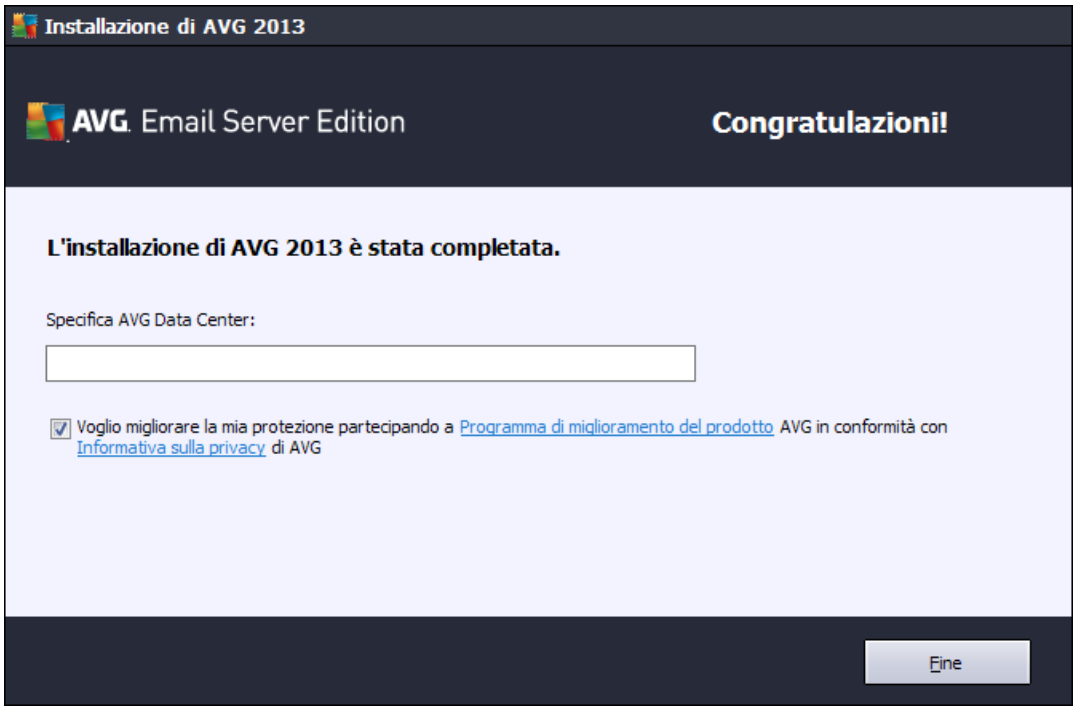
  Controlla tutti i messaggi email archiviati nelle cassette postali degli utenti. Se vengono rilevati virus, questi vengono spostati in quarantena o completamente rimossi.

Per gli utenti Exchange 2003 sono disponibili solo i componenti Anti-Spam e Scansione Email (VSAPI).

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

3.6. Completamento dell'installazione

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



Questa finestra di dialogo consente di scegliere se partecipare al Programma di miglioramento del prodotto che raccoglie informazioni anonime sulle minacce rilevate per aumentare il livello globale di protezione in Internet. In caso di accordo, mantenere l'opzione ***Desidero migliorare la protezione in uso partecipando al Programma di miglioramento del prodotto in conformità con l'informativa sulla privacy di AVG*** selezionata *(l'opzione viene confermata per impostazione predefinita)*.

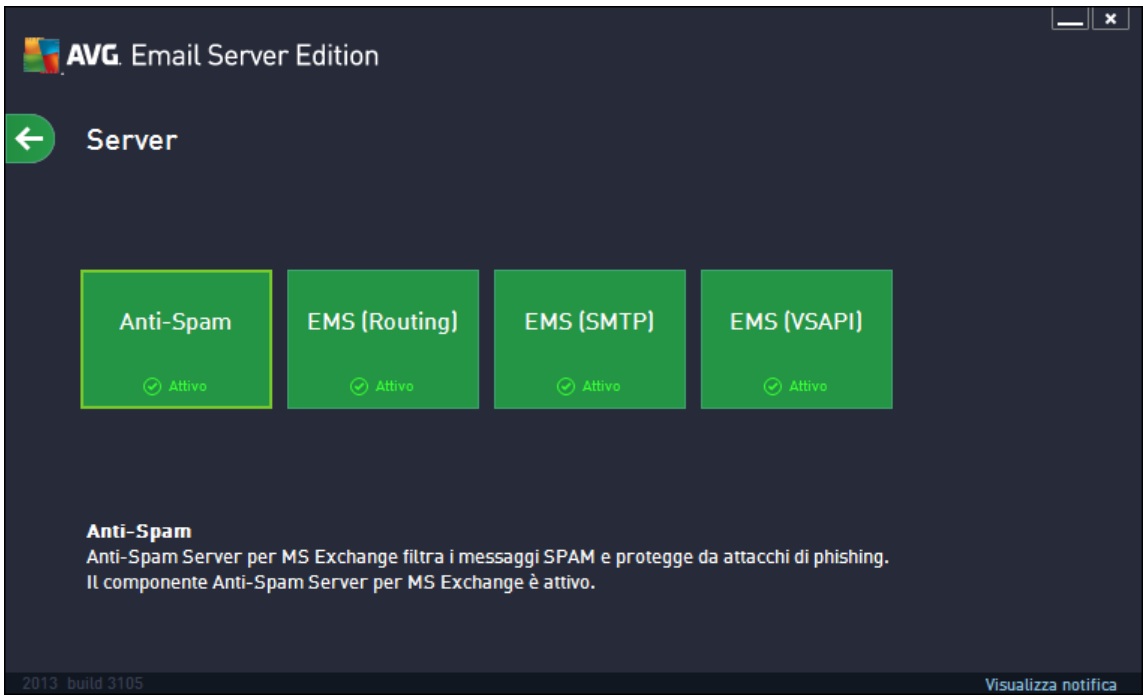
Confermare la selezione facendo clic sul pulsante **Fine**.

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

4. Dopo l'installazione

Subito dopo aver completato l'installazione, verrà visualizzata la schermata principale ***AVG Email Server Edition 2013***:

Questo manuale si riferisce solo alle funzionalità specifiche di ***AVG Email Server Edition 2013***. Tutti gli altri componenti e le altre impostazioni vengono descritti nel manuale desktop di AVG. Per accedere alla finestra di dialogo dei principali componenti server, fare clic sul pulsante ***Server***. Verrà visualizzata la seguente finestra:



I componenti server saranno tutti disponibili (se non si è scelto di non installarne alcuni durante il processo di installazione) solo se si utilizza MS Exchange 2007 o una versione successiva. MS Exchange 2003 supporta solo i componenti Anti-Spam e Scansione Email(VSAPI).

Per configurare la protezione individualmente per il server email, consultare il capitolo appropriato:

- ***Scansione Email per MS Exchange***
- ***Anti-Spam Server per MS Exchange***
- ***AVG per Kerio MailServer***

5. Scansione E-mail per MS Exchange

5.1. Panoramica

Panoramica di base dei singoli componenti server di Scansione Email:

- ***EMS (routing): Scansione Email per MS Exchange (routing Transport Agent)***

  Controlla tutti i messaggi email 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 Email per MS Exchange (SMTP Transport Agent)***

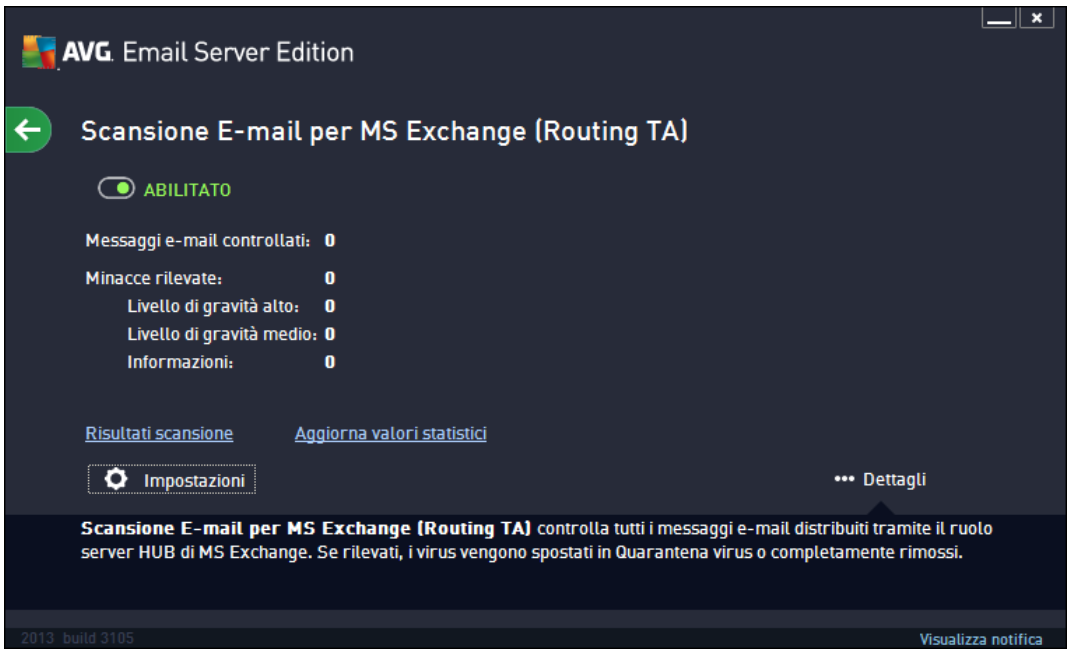
  Controlla tutti i messaggi email ricevuti tramite l'interfaccia MS Exchange SMTP.

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

- ***EMS (VSAPI): Scansione Email per MS Exchange (VSAPI)***

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

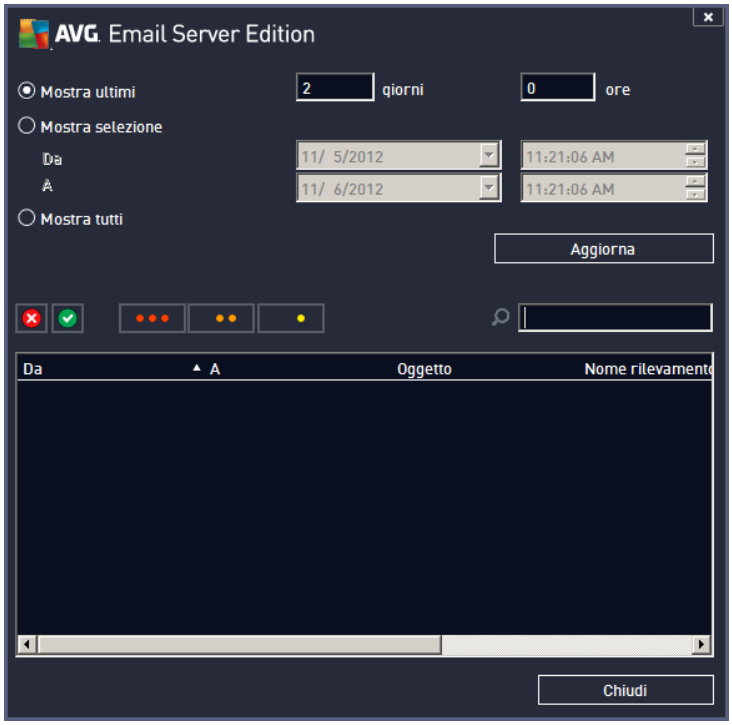
Fare clic sull'icona del componente desiderato per aprirne l'interfaccia. Tutti i componenti condividono i seguenti pulsanti di controllo e collegamenti comuni:



- ***ATTIVATO/DISATTIVATO***: questo pulsante consente di attivare o disattivare il componente selezionato (quando il componente è attivo il pulsante e il testo sono verdi; in caso contrario, sono rossi).

- ***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.

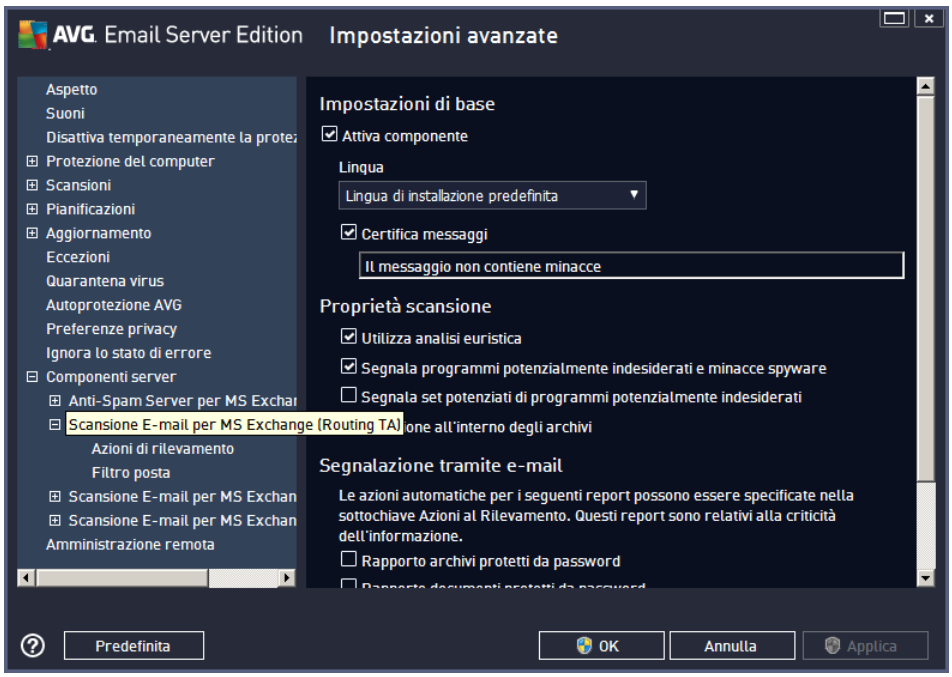
- ***Aggiorna valori statistici***: aggiorna le statistiche visualizzate in alto.

Facendo clic sul pulsante ***Impostazioni*** si apriranno le impostazioni avanzate per il componente selezionato (nei seguenti capitoli sono disponibili ulteriori informazioni sulle impostazioni specifiche di tutti i componenti).

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

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

Dall'elenco ***Componenti server*** selezionare la voce ***Scansione Email 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 ***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 email*** consente di scegliere quali elementi devono essere segnalati

durante la scansione. Se questa opzione è selezionata, ciascuna email 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 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***

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

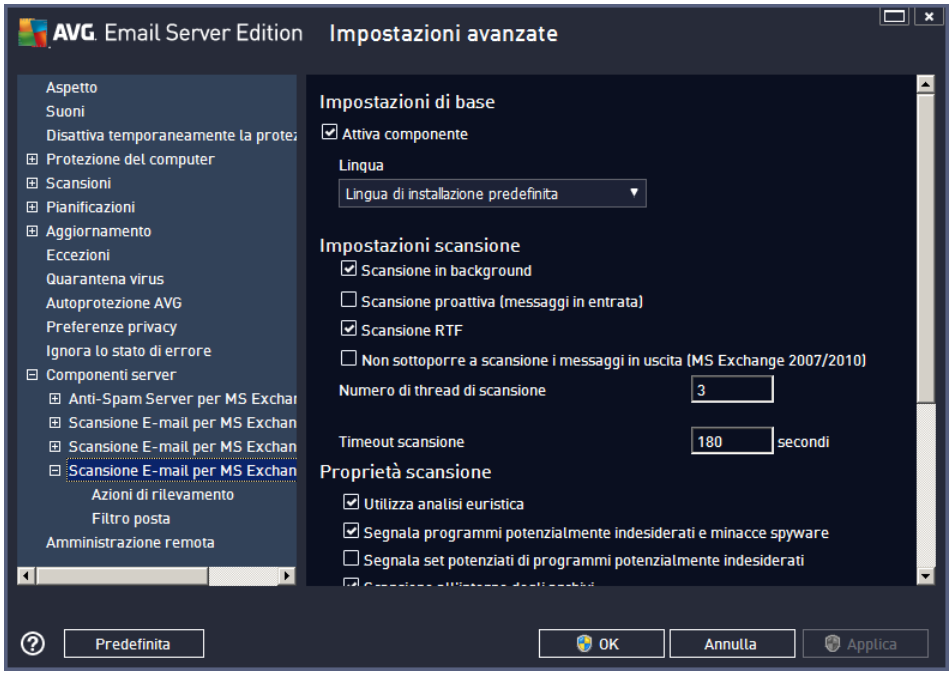
La configurazione di ***Scansione Email per MS Exchange (SMTP Transport Agent)*** è esattamente uguale in caso di routing transport agent. Per ulteriori informazioni consultare il capitolo precedente ***Scansione Email per MS Exchange (routing TA)***.

Sono inoltre disponibili le presenti sottovoci nella seguente struttura:

- ***Azioni di rilevamento***
- ***Filtro posta***

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

Questa voce contiene le impostazioni di ***Scansione Email 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 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 di bassa priorità viene utilizzato per ciascun database, in modo da garantire che altre attività (ad esempio l'archiviazione di messaggi email nel database Microsoft Exchange) vengano 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.

I messaggi di overflow continueranno ad essere memorizzati senza essere sottoposti a scansione.

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.
- ***Non sottoporre a scansione i messaggi in uscita (MS Exchange 2007/2010)***: se sono stati installati entrambi i componenti server VSAPI e Routing Transport Agent (Routing TA), indipendentemente dal fatto che questi si trovino su un unico server o su due server diversi, la posta in uscita potrebbe venire sottoposta a scansione due volte. La prima scansione viene effettuata all'accesso da VSAPI, la seconda da Routing Transport Agent. Ciò potrebbe causare rallentamenti dei server e ritardi nell'invio dei messaggi email. Se si è certi che entrambi i componenti server sono installati e attivi, è possibile evitare il doppio controllo delle email in uscita selezionando questa casella e disattivando la scansione all'accesso di VSAPI.
- ***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 email*** 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***

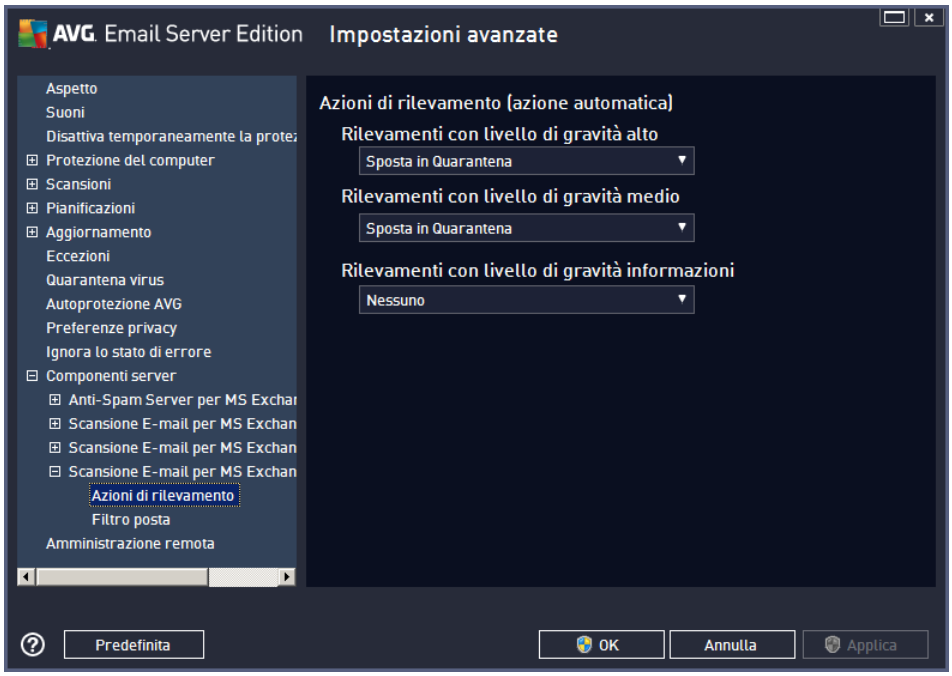
In genere, alcune di queste funzioni sono estensioni per l'utente dei servizi dell'interfaccia applicativa Microsoft VSAPI 2.0/2.5. Per informazioni dettagliate su VSAPI 2.0/2.5, vedere i seguenti collegamenti e i collegamenti accessibili tramite essi:

- 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***

5.5. 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:

- ***Rilevamenti con livello di gravità alto***: codice dannoso che viene copiato e diffuso automaticamente, spesso in modo nascosto fino a quando il danno è evidente.
- ***Rilevamenti con livello di gravità medio***: in linea generale variano da minacce effettivamente pericolose a minacce solo potenziali con effetto sulla privacy.
- ***Rilevamenti con livello di gravità informazioni***: include tutte le minacce potenziali rilevate che non possono essere classificate in una delle categorie precedenti.

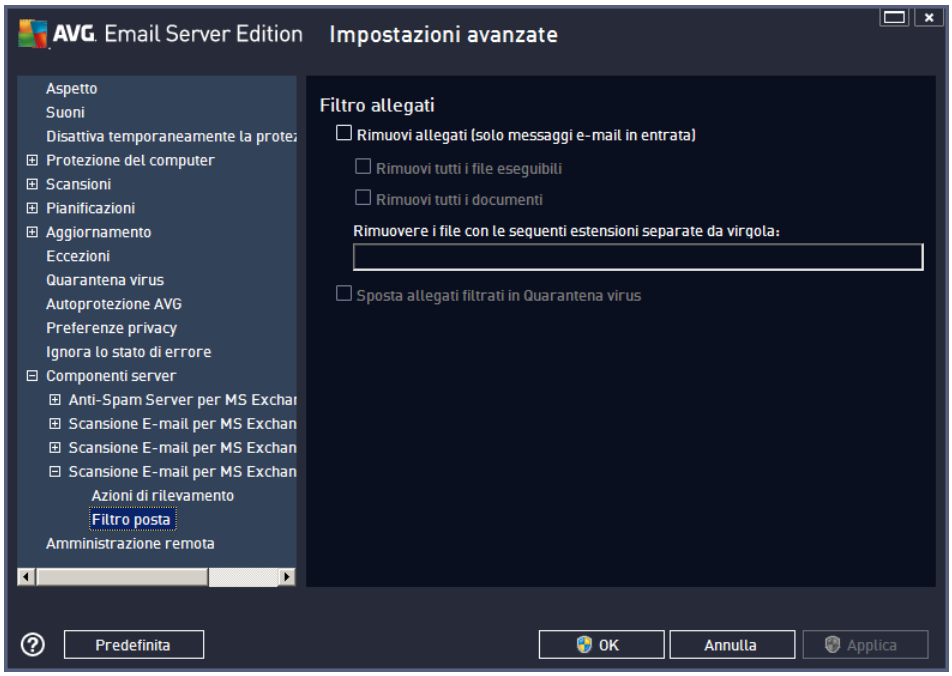
Utilizzare il menu a discesa per selezionare un'azione per ciascuna voce:

- ***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.

L'ultima funzione citata non è disponibile per Scansione Email per MS Exchange (VSAPI).

5.6. 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.
- ***Sposta allegati filtrati in Quarantena virus***: selezionare la casella se non si desidera che gli allegati filtrati vengano rimossi completamente. Se questa casella è selezionata, tutti gli allegati scelti in questa finestra di dialogo verranno automaticamente spostati in Quarantena virus. Quarantena virus è un'area sicura in cui vengono memorizzati i file potenzialmente pericolosi, che possono quindi essere aperti ed esaminati senza rappresentare rischi per il sistema. È possibile accedere a Quarantena virus dal menu superiore dell'interfaccia principale di **AVG Email Server Edition 2013**. È sufficiente fare clic sull'elemento ***Opzioni*** e scegliere la voce ***Quarantena virus*** dal menu a discesa.

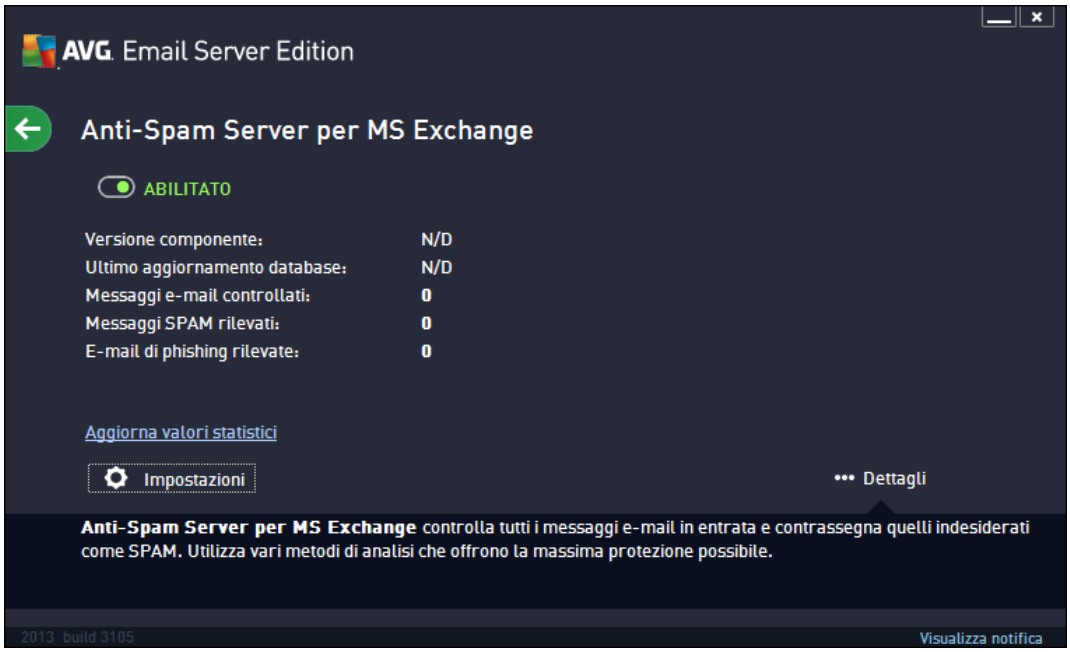
6. Anti-Spam Server per MS Exchange

6.1. Principi dell'Anti-Spam

Il termine "spam" indica messaggi email indesiderati, per lo più pubblicità di prodotti o servizi, inviati in massa e simultaneamente a un enorme numero di indirizzi email, che intasano le cassette postali dei destinatari. Lo spam non rientra nella categoria dei messaggi email commerciali legittimi 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 email in entrata e contrassegna i messaggi indesiderati come SPAM. Per elaborare ogni messaggio email vengono utilizzati diversi metodi di analisi che offrono il massimo livello di protezione possibile contro i messaggi email indesiderati.

6.2. Interfaccia dell'Anti-Spam



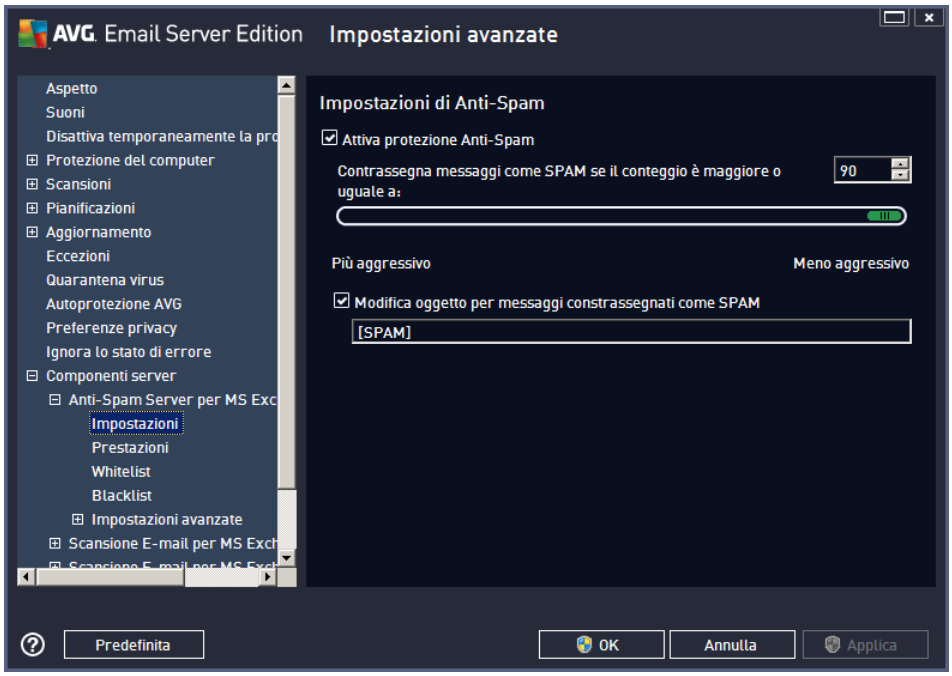
Questa finestra di dialogo include brevi informazioni sulle funzionalità e lo stato corrente del componente server (*Attivato/Disattivato*) e alcuni dati statistici.

Collegamenti e pulsanti disponibili:

- ***ATTIVATO/DISATTIVATO***: questo pulsante consente di attivare o disattivare il componente selezionato (quando il componente è attivo il pulsante e il testo sono verdi; in caso contrario, sono rossi).
- ***Aggiorna valori statistici***: aggiorna le statistiche visualizzate in alto.
- ***Impostazioni***: selezionare questo pulsante per aprire le impostazioni avanzate dell'Anti-Spam.

6.3. Impostazioni dell'Anti-Spam

6.3.1. Impostazioni



In questa finestra di dialogo è possibile selezionare la casella di controllo ***Attiva protezione Anti-Spam*** per consentire/impedire la scansione anti-spam delle comunicazioni email.

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:

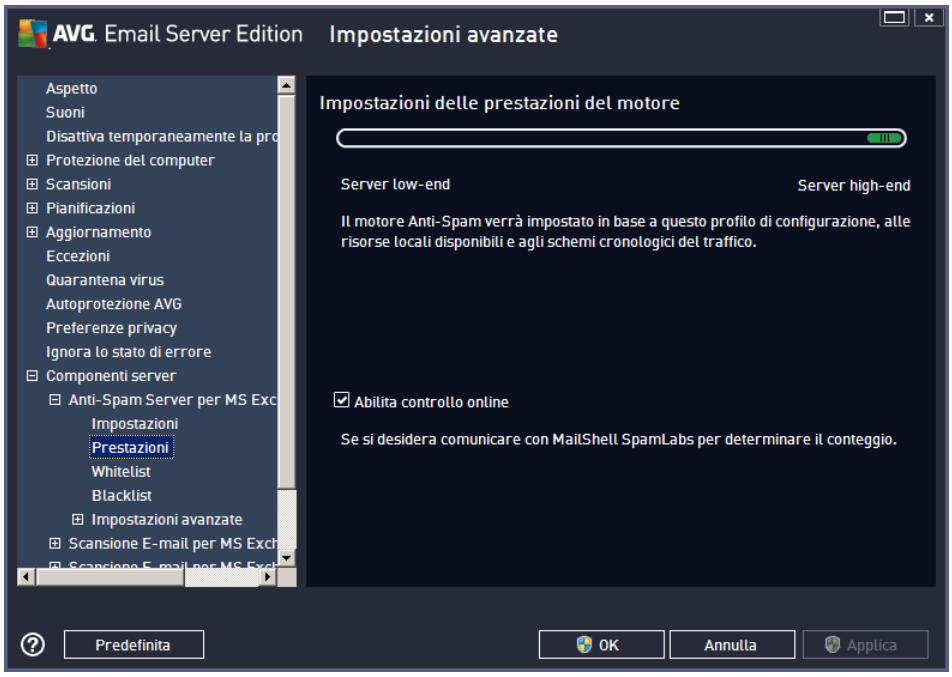
- ***Valore 90***: la maggior parte dei messaggi email in entrata verrà recapitata normalmente (senza venire contrassegnata come spam). Lo spam più facilmente identificato verrà filtrato, tuttavia si potrebbe ricevere comunque una notevole quantità di spam.
- ***Valore compreso tra 80 e 89***: verranno filtrati i messaggi email 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 considerati potenzialmente spam. È possibile che vengano filtrati anche alcuni messaggi normali.
- ***Valore compreso tra 50 e 59***: configurazione particolarmente aggressiva. È probabile che insieme ai messaggi email contenenti spam vengano filtrati anche i messaggi normali. Questo intervallo di valori non è consigliato per l'uso normale.

È possibile definire ulteriormente il modo in cui trattare i messaggi email 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 email; il testo desiderato può essere digitato nel campo di testo attivato.

- ***Chiedi conferma prima di segnalare rilevamenti errati***: se durante il processo di installazione si è scelto di partecipare al programma di miglioramento del prodotto (che consente ad AVG di raccogliere informazioni aggiornate fornite dagli utenti in tutto il mondo sulle minacce più recenti e di migliorare la protezione in rete per tutti), ovvero si è acconsentito a segnalare ad AVG le minacce rilevate. La segnalazione viene effettuata automaticamente. È tuttavia possibile selezionare questa casella di controllo per specificare se si desidera che venga richiesta una conferma prima della segnalazione ad AVG dell'eventuale spam rilevato, in modo da assicurarsi che il messaggio debba effettivamente essere classificato come spam.

6.3.2. 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

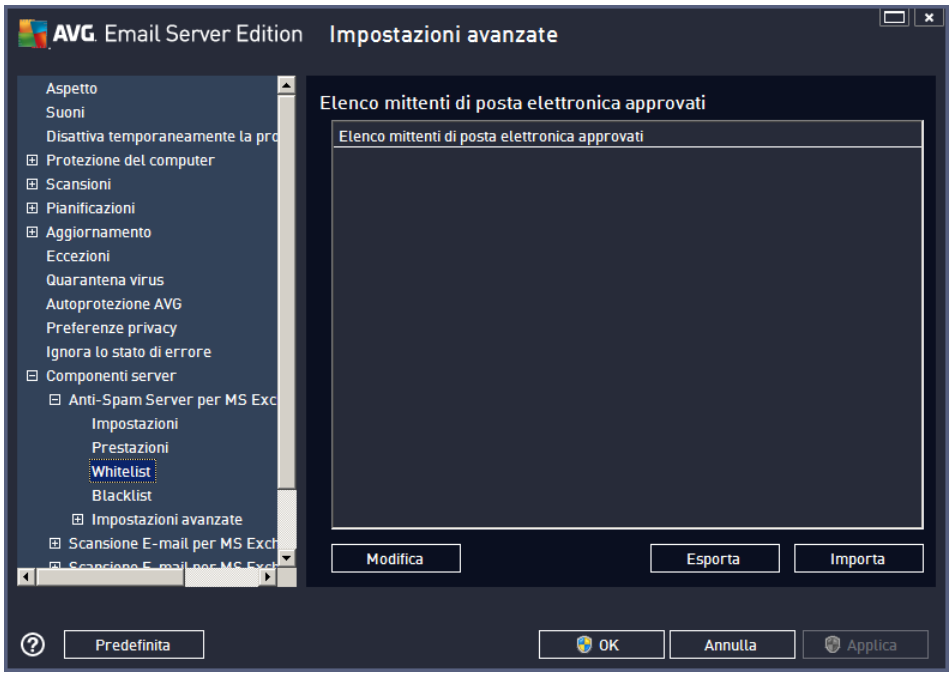
database di spammer.

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

6.3.3. Whitelist

La voce ***Whitelist*** consente di aprire una finestra di dialogo con un elenco globale di indirizzi di mittenti email 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 email o importando tutto l'elenco di indirizzi. Sono disponibili i seguenti pulsanti di controllo:

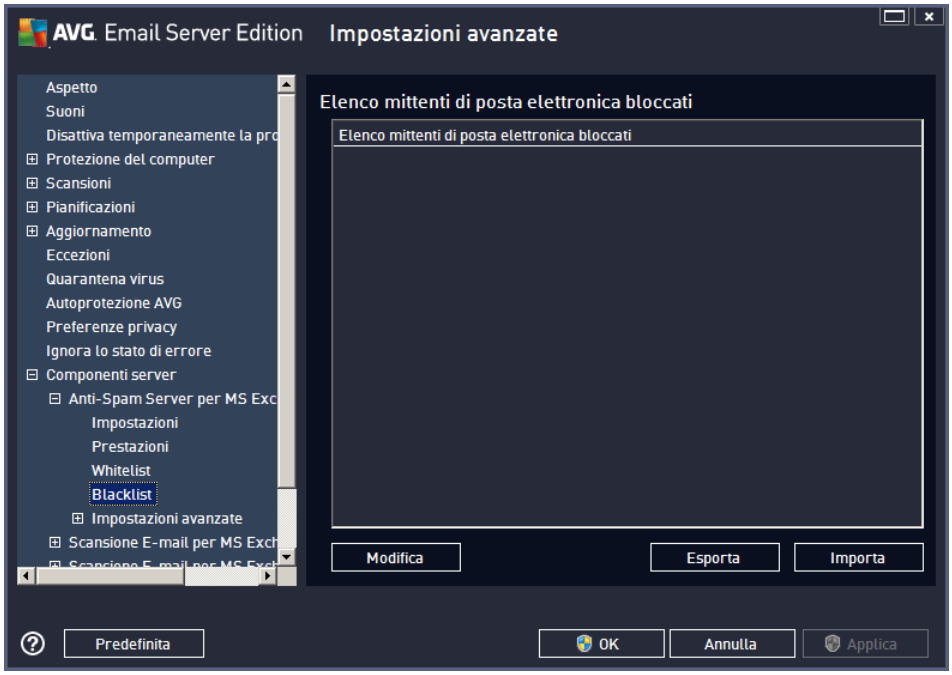
- ***Modifica***: selezionare questo pulsante per aprire una finestra di dialogo in cui è possibile immettere manualmente un elenco di indirizzi (è inoltre possibile utilizzare il metodo *copia e incolla*). Immettere una voce (mittente o nome di dominio) per riga.

- ***Importa***: è possibile importare gli indirizzi email 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.

6.3.4. Blacklist

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



Nell'interfaccia di modifica è possibile compilare un elenco di mittenti da cui si ha la certezza di ricevere messaggi indesiderati (spam). È inoltre possibile compilare un elenco di nomi di dominio completi (ad esempio *aziendaspam.com*), da cui si prevede di ricevere o si ricevono messaggi di spam. Tutti i messaggi email ricevuti da tali indirizzi o domini specifici verranno considerati 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 email 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 email esistenti selezionando questo pulsante. Il file di input può essere un file di testo in formato testo normale, il cui 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.

6.3.5. Impostazioni avanzate

Questo ramo contiene ampie opzioni di impostazione per il componente Anti-Spam. Queste impostazioni sono destinate esclusivamente agli utenti esperti, in particolare agli amministratori di rete che devono eseguire una configurazione dettagliata della protezione anti-spam per garantire la massima protezione dei server email. Per questo motivo non è disponibile una guida aggiuntiva nelle singole finestre di dialogo. Tuttavia, è disponibile direttamente nell'interfaccia utente una breve descrizione di ciascuna opzione.

Si consiglia di non modificare alcuna impostazione a meno che non si abbia familiarità con tutte le impostazioni avanzate di Spamcatcher (MailShell Inc.). Eventuali modifiche inappropriate possono dare luogo a una riduzione delle prestazioni o a un funzionamento errato del componente.

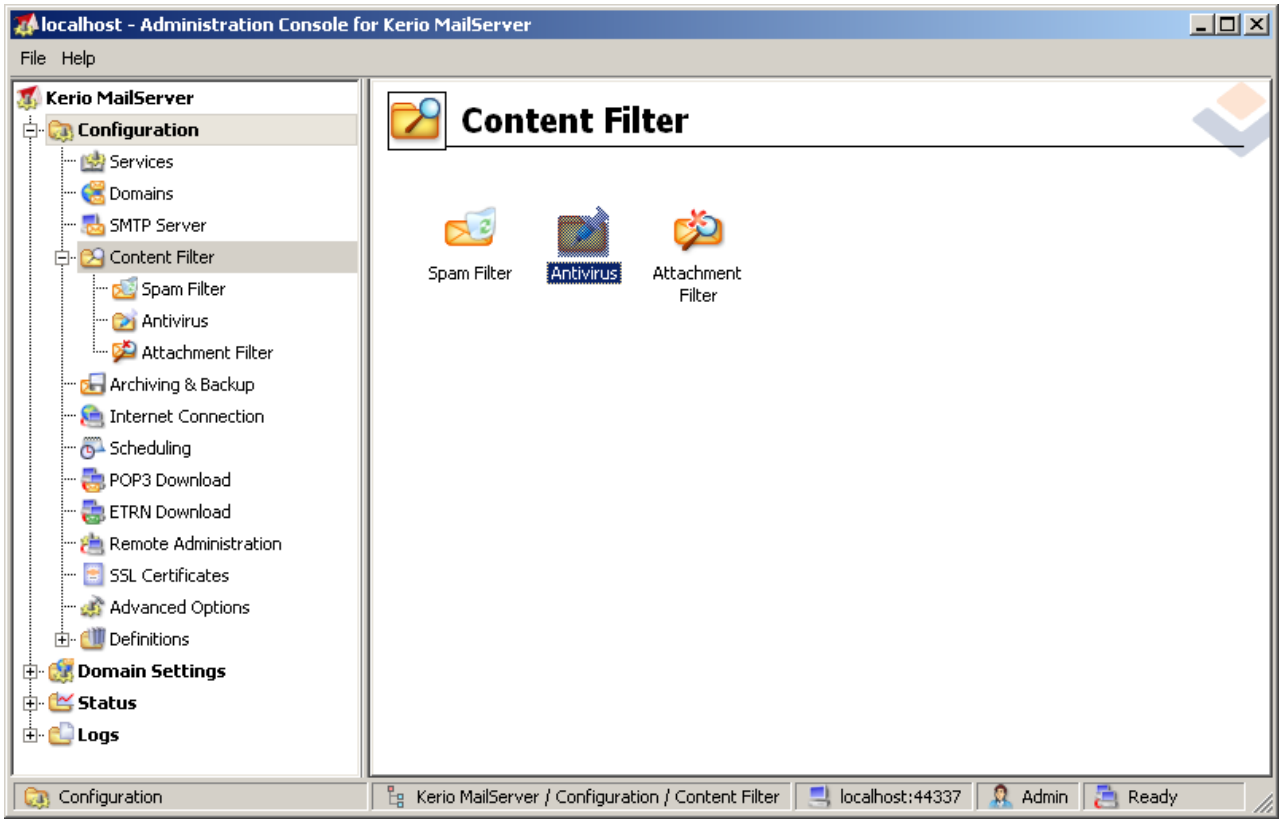
Se si ritiene di dover modificare comunque la configurazione del componente Anti-Spam a un livello molto avanzato, seguire le istruzioni fornite direttamente nell'interfaccia utente. In genere, in ciascuna finestra di dialogo è contenuta una sola funzionalità specifica che può essere modificata. La descrizione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

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

7. AVG per Kerio MailServer

7.1. Configurazione

Il meccanismo di protezione antivirus è integrato direttamente nell'applicazione Kerio MailServer. Per attivare la protezione dei messaggi email di Kerio MailServer tramite il 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:

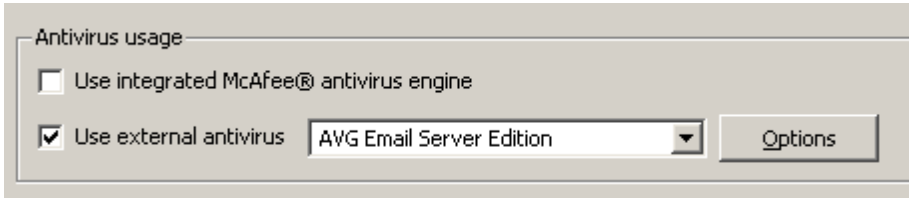


Se si fa clic su Filtro contenuti viene visualizzata la finestra di dialogo con i tre elementi:

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

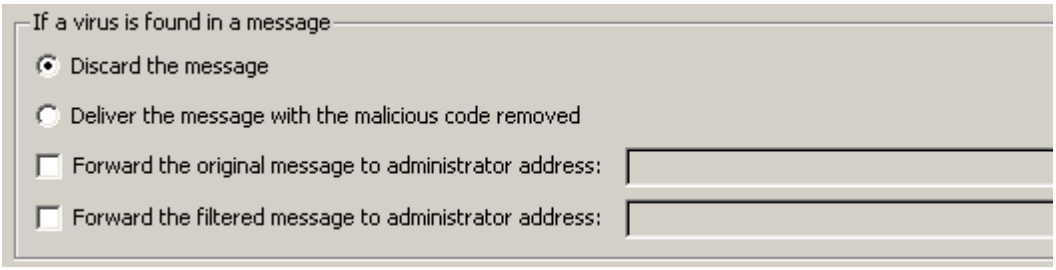
7.1.1. Antivirus

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:

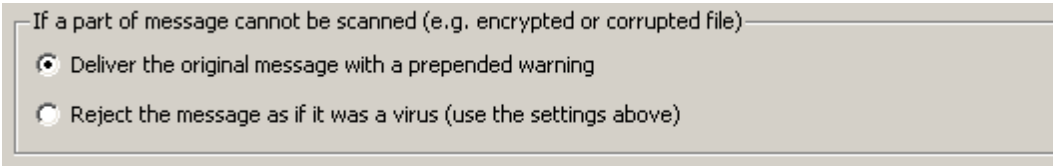
- ***Se viene rilevato un virus in un messaggio***



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)***



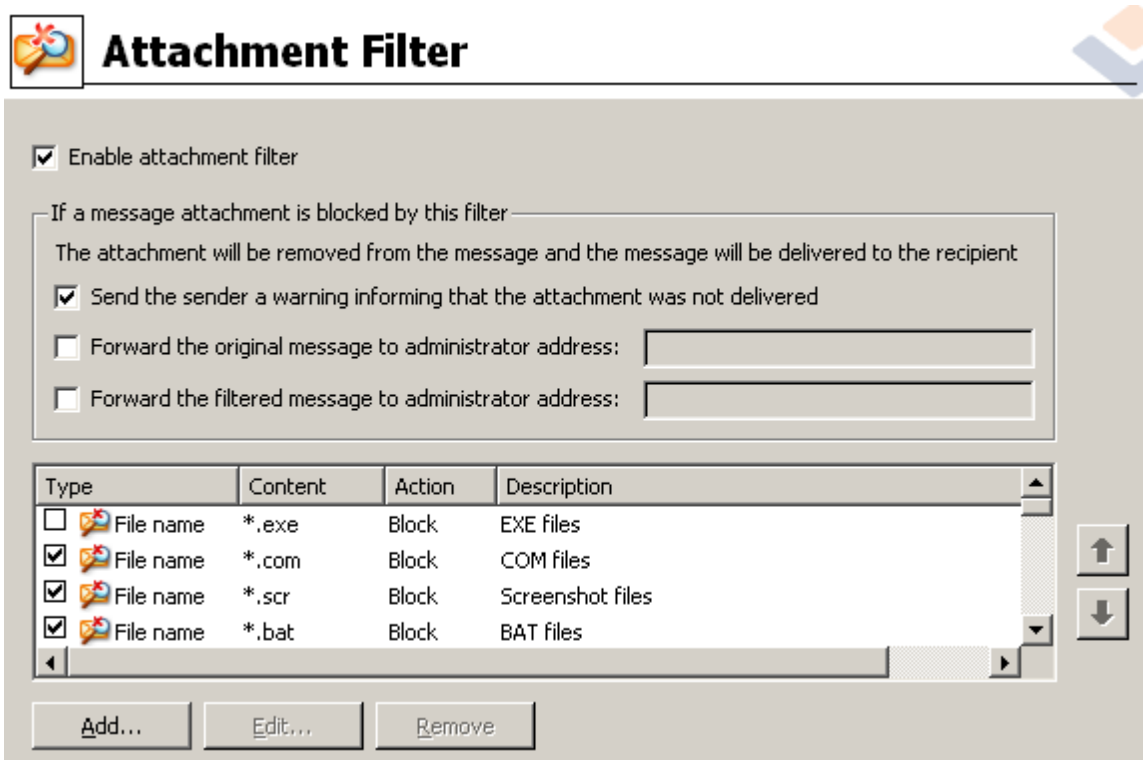
Questo frame consente di specificare l'azione da eseguire se non è possibile esaminare una parte del messaggio o dell'allegato:

  - ***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.

7.1.2. Filtro allegati

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



È possibile attivare o disattivare il filtro degli allegati email 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 email 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 email 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.

8. 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 email. Utilizzare il modulo di contatto accessibile dal menu di sistema tramite ***Guida in linea / Utilizza Guida in linea***.