GFI MailEssentials 14.1

Manuale di amministrazione e configurazione

A cura di GFI Software Ltd.

http://www.gfi.com
E-mail: info@gfi.com

Versione ME-ACM-IT-1-02.003

Ultimo aggiornamento: 19 ottobre 2009

Indice

1 Informazioni su GFI MailEssentials

1.1 Introduzione

GFI MailEssentials è una soluzione antispam basata su server che offre al proprio server di posta importanti funzioni contro lo spam della posta elettronica aziendale. Installato come un'aggiunta al proprio server di posta, GFI MailEssentials è completamente trasparente per gli utenti, i quali non devono partecipare ad alcun corso di formazione supplementare.

Le funzioni principali di questa soluzione sono le seguenti:

- **Antispam basato su server** - La protezione dallo spam è una componente essenziale della strategia di sicurezza della rete. GFI MailEssentials fornisce filtri antispam avanzati che comprendono black list/white list, filtraggio bayesiano, verifica delle parole chiave e analisi delle intestazioni.
- **Declinazione di responsabilità/testo a piè di pagina a livello aziendale** - Le aziende sono responsabili del contenuto dei messaggi di posta elettronica dei propri dipendenti. GFI MailEssentials consente di aggiungere in modo automatico la declinazione di responsabilità in alto o in basso di un messaggio di posta elettronica con la possibilità di personalizzare la declinazione di responsabilità in funzione del destinatario grazie ai campi e alle variabili.
- **Archiviazione dei messaggi di posta elettronica in un data base** - L'archiviazione dei messaggi posta elettronica costituisce non solo una buona prassi, ma può essere anche un requisito ai sensi di legge. GFI MailEssentials offre lo strumento che consente di archiviare tutti i messaggi di posta elettronica in arrivo e in uscita.
- **Rapporti** - GFI Mail Essentials può produrre vari rapporti utili sull'uso dei messaggi di posta elettronica e sulle operazioni antispam.
- **Risposte automatiche personalizzate con numero di tracciabilità** - Più di semplici risposte "fuori sede", le risposte automatiche consentono ai clienti di sapere che i propri messaggi di posta elettronica sono stati ricevuti e che la richiesta viene gestita. È possibile assegnare un numero di tracciabilità esclusivo a ogni risposta per dare a clienti e dipendenti un facile punto di riferimento.
- ***Downloader* POP3 -** Le aziende più piccole possono non avere gli strumenti necessari per usare la posta elettronica basata su SMTP. GFI MailEssentials comprende un programma di utilità in grado di inoltrare e distribuire messaggi di posta elettronica da cassette postali POP3 a cassette postali sul server di posta.

- **Monitoraggio dei messaggi di posta elettronica** - Gli archivi di informazioni centrali sono in genere più facili da gestire rispetto alle informazioni distribuite. GFI MailEssentials consente l'invio di copie dei messaggi di posta elettronica a un archivio centrale delle comunicazioni via posta elettronica di una certa persona o di un reparto specifico.

Per maggiori informazioni sulla modalità di filtraggio di GFI MailEssentials dei messaggi di posta elettronica in arrivo e in uscita, consultare Appendice 1 - Modalità di funzionamento del filtraggio antispam del presente manuale.

1.2 Uso del presente manuale

Questo manuale dell'utente è una guida completa intesa ad assistere gli amministratori dei sistemi nella configurazione e nell'utilizzo di GFI MailEssentials nel miglior modo possibile. Sviluppa le istruzioni fornite nella "Guida introduttiva" di GFI MailEssentials e descrive le impostazioni di configurazione raccomandate agli amministratori dei sistemi per ottenere i migliori risultati possibili dal software.

Il presente manuale contiene i seguenti capitoli:

Capitolo 1	Introduce questo manuale.
Capitolo 2	Fornisce informazioni dettagliate sui compiti amministrativi consueti che gli amministratori devono svolgere quotidianamente.
Capitolo 3	Contiene informazioni dettagliate sulla modalità di personalizzazione di GFI MailEssentials. È possibile personalizzare filtri antispam e azioni associate, nonché declinazioni di responsabilità e risposte automatiche.
Capitolo 4	Fornisce informazioni dettagliate sulla modalità di esecuzione di altri compiti di manutenzione e configurazione non trattati nei due capitoli precedenti. Tali compiti comprendono la configurazione della funzione P2E, il monitoraggio dei messaggi di posta elettronica e i comandi a distanza.
Capitolo 5	Una sezione dedicata alla risoluzione dei problemi e all'assistenza dove vengono date informazioni per risolvere i problemi comuni.
Appendici	Offre informazioni supplementari riguardanti il modo di lavorare del filtraggio di spam e del filtraggio bayesiano e informazioni su MSMQ.

1.3 Licenze

Per le informazioni riguardanti le licenze, consultare:

http://www.gfi.com/products/gfi-mailessentials/pricing/licensing

1.4 Requisiti minimi e installazione

Per maggiori informazioni sui requisiti di sistema e sull'installazione, consultare la "Guida introduttiva" di GFI MailEssentials:

http://www.gfi-italia.com/it/me/mes14gsgmanual_it.pdf

2 Azioni raccomandate dopo l'installazione

2.1 Introduzione

Filtri antispam

Alla consegna, GFI MailEssentials comprende alcuni filtri antispam specifici. Ciascuno di questi filtri è specifico per uno o più tipi di spam. I filtri spediti con GFI MailEssentials sono elencati qui di seguito:

Filtro	Descrizione	Attivato per impostazione predefinita
SpamRazer	Un motore antispam che stabilisce se un messaggio di posta elettronica è uno spam utilizzando la reputazione dei messaggi, le impronte digitali dei messaggi e l'analisi dei contenuti.	Si
Raccolta di directory	Blocca un messaggio di posta elettronica che viene casualmente generato verso un server e inviato prevalentemente a utenti non esistenti.	Si
Phishing	Blocca i messaggi di posta elettronica contenenti nel corpo del messaggio link a siti di phishing noti o parole chiave tipiche dell'attività di phishing.	Si
Sender Policy Framework	Ferma messaggi di posta elettronica provenienti da domini non autorizzati secondo i registri Sender Policy Framework.	No
White list automatica	Gli indirizzi a cui un messaggio di posta elettronica viene inviato sono automaticamente esclusi dal blocco.	Si
White list	Un elenco personalizzato di indirizzi di posta elettronica sicuri.	Si
Black list dei messaggi di posta elettronica	Un elenco personalizzato di utenti o domini di posta elettronica bloccati.	Si
Black list DNS	Verifica se il messaggio di posta elettronica proviene dai mittenti presenti in una black list DNS pubblica di spammer noti.	Si
Block list di URI anti-spam in tempo reale	Ferma messaggi di posta elettronica che contengono link a domini presenti su Blocklist antispam di URI pubbliche come sc.surbl.org.	Si
Controllo intestazioni	Un modulo che analizza i singoli campi di un'intestazione relazionandoli ai campi SMTP e MIME.	Si

Controllo parola chiave	I messaggi di spam sono individuati sulla base di parole chiave bloccate nel titolo o nel corpo del messaggio di posta elettronica.	No
Nuovi mittenti	Messaggi di posta elettronica ricevuti da mittenti a cui non erano mai stati inviati messaggi prima d'ora.	No
Analisi bayesiana	Tecnica antispam dove viene creato un indice di probabilità statistica basata sulle informazioni utente.	No

Tabella 1 - Filtri antispam abilitati per impostazione predefinita

Come descritto nella tabella in alto, non tutti i filtri antispam sono attivati per impostazione predefinita. Ciò è dovuto alle impostazioni di configurazione che dipendono dalla rete/infrastruttura e non possono pertanto essere preimpostate. Sebbene i filtri principali come SpamRazer siano abilitati per impostazione predefinita, si raccomanda di rivedere e abilitare, dopo aver installato GFI MailEssentials, il resto dei filtri antispam e i meccanismi di filtraggio. Per maggiori informazioni, consultare il capitolo Filtri antispam a pagina 32 del presente manuale.

Azioni antispam

Alcune azioni possono essere avviate dai filtri antispam quando viene rilevato un messaggio di spam. Tali azioni stabiliscono cosa fare dello spam rilevato e sono configurabili filtro per filtro. Le azioni dei filtri antispam supportate sono le seguenti:

- Etichettare il messaggio di spam (impostazione predefinita)
- Spostare il messaggio di spam verso una cartella centrale
- Spostare il messaggio di spam verso cartelle pubbliche
- Spostare il messaggio di spam verso una cartella di posta indesiderata
- Inoltrare il messaggio di spam a un indirizzo di posta elettronica specifico.
- Eliminare lo spam

Azioni antispam predefinite

L'azione predefinita eseguita quando GFI MailEssentials blocca un messaggio di spam, dipende da dove è installato il software:

Distribuzione	Azione predefinita	Descrizione
GFI MailEssentials intallato sullo stesso computer di Microsoft Exchange	Consegna il messaggio alla sottocartella della cassetta postale di Exchange	Quando un filtro blocca un messaggio di spam, il messaggio di posta viene spostato in una sottocartella della Posta in arrivo denominata Presunto spam.
GFI MailEssentials non installato sullo stesso computer di Microsoft Exchange	Etichettatura	I filtri antispam aggiungono il prefisso [SPAM] nel campo dell'oggetto dei messaggi di spam. I messaggi di posta etichettati sono comunque consegnati nella Posta in arrivo dell'utente.

Per maggiori informazioni sulle azioni antispam, consultare la sezione Azioni antispam: cosa fare dei messaggi di spam a pagina 73 del presente manuale.

2.2 Indirizzare lo spam verso cartelle di spam dedicate

Per evitare che lo spam venga inviato alla Posta in arrivo dei destinatari, è possibile configurare GFI MailEssentials per indirizzare i messaggi di spam verso cartelle di spam dedicate. L'utente può configurare una cartella di spam specifica per ogni filtro antispam, potendo in questo modo dividere lo spam in categorie e sapere quale filtro abbia bloccato lo spam. Si tratta di una funzione importante per individuare messaggi ingannevoli e modificare i filtri di conseguenza.

Indirizzare messaggi di spam verso apposite cartelle

Varie azioni antispam "spostare nella cartella" sono disponibili a seconda della tipologia di configurazione a disposizione.

Con un'infrastruttura Microsoft Exchange 2003/2007/2010, è possibile avviare le seguenti azioni "spostare nella cartella":

- **Nella Posta in arrivo** - Usare questa opzione per indirizzare lo spam nella Posta in arrivo dell'utente.
- **Nella cartella di posta indesiderata di Exchange** - Usare questa opzione per indirizzare tutto lo spam verso la cartella predefinita destinata ai messaggi indesiderati dell'utente.
- **Nella sottocartella della cassetta postale di Exchange** - Usare questa opzione per indirizzare tutto lo spam verso una cartella specifica nella cassetta postale dell'utente.

Su altre infrastrutture, l'utente può indirizzare i messaggi di spam verso una cartella specifica del client/dell'utente finale.

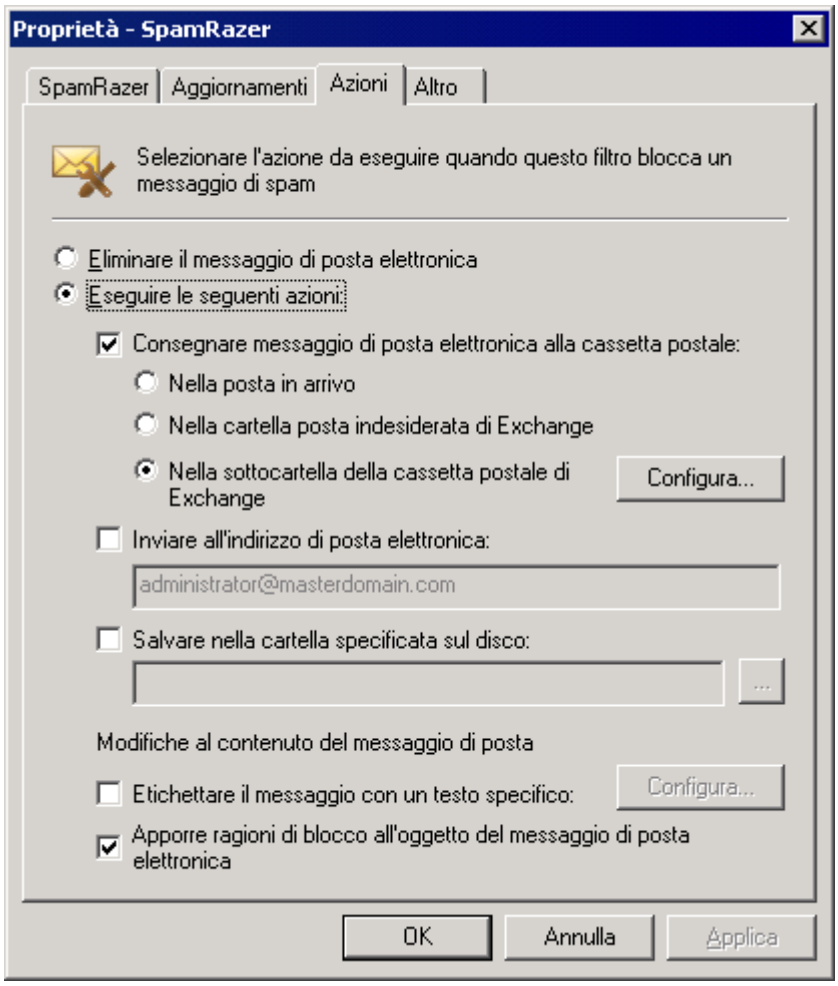
2.2.1 Configurazione dell'inoltro di messaggi di posta elettronica verso apposite cartelle

NOTA: questa sezione è applicabile quando GFI MailEssentials è installato esclusivamente nello stesso server in cui risiede Microsoft Exchange Server. Se GFI MailEssentials è installato su un altro computer fare riferimento alla sezione Spostamento dei messaggi di spam nelle cartelle della cassetta postale dell'utente a pagina 122 di questo manuale

1. GFI MailEssentials configuration può essere lanciata cliccando:

Start ► Tutti i programmi ► GFI MailEssentials ► GFI MailEssentials Configuration.

2. Dall'elenco dei filtri, fare clic con il pulsante destro del mouse sul nodo **Antispam ► Filtri antispam** per la configurazione, per es., **Controllo intestazioni** e selezionare **Proprietà.**



Schermata 1 - Configurazione dell'azione da intraprendere

3. Fare clic sulla scheda **Azioni** per accedere alle opzioni relative alla configurazione delle azioni dei filtri antispam.

4. Selezionare **Consegna il messaggio di posta elettronica nella cassetta postale** e scegliere una delle seguenti opzioni:

- **Nella posta in arrivo** - Usare questa opzione per indirizzare lo spam nella Posta in arrivo dell'utente.
- **Nella cartella di posta indesiderata di Exchange** - Usare questa opzione per indirizzare tutto lo spam verso la cartella predefinita Posta Indesiderata dell'utente.
- **Nella sottocartella della cassetta postale di Exchange** - Usare questa opzione per indirizzare tutto lo spam verso una cartella specifica nella cassetta postale dell'utente. Fare clic su **Configura** per avviare la finestra di dialogo **Sposta nella cartella Exchange** e digitare la cartella nella quale spostare il messaggio di spam.

  Esempio: "Posta in arrivo\Posta spam" creerà una sottocartella chiamata Posta spam nella Posta in arrivo.

5. Fare clic su **OK** per salvare la configurazione.

6. Ripetere per tutti i filtri spam abilitati.

2.3 Abilitazione della scansione della cartella pubblica

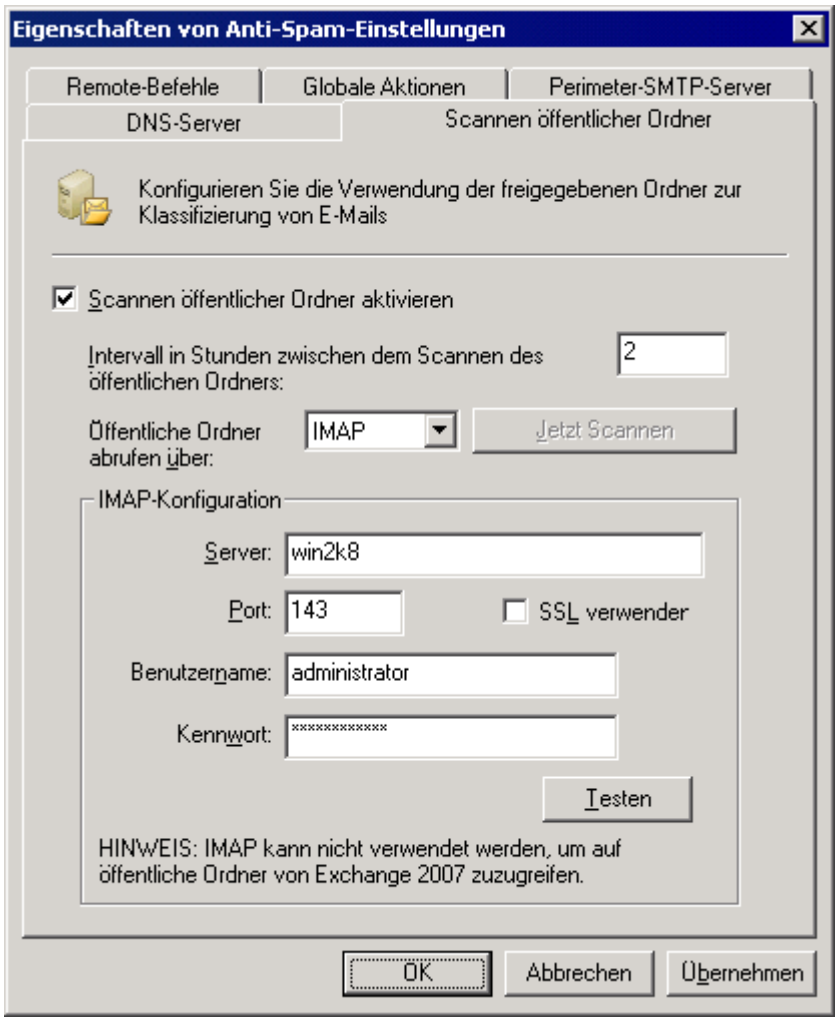
Le tecniche di spamming sono in continua evoluzione; di conseguenza, potrebbero presentarsi casi in cui un messaggio di spam riesca a eludere i filtri antispam e a raggiungere la Posta in arrivo del destinatario. Mediante la scansione della cartella pubblica, gli utenti possono classificare manualmente i messaggi di posta elettronica come spam e "insegnare" ai modelli spam di GFI MailEssentials a classificare messaggi di posta elettronica analoghi come spam.

La scansione della cartella pubblica consente a GFI MailEssentials di recuperare i messaggi di posta elettronica dalle cartelle pubbliche per aggiungerli a white list/black list e data base HAM/SPAM. Sui sistemi dotati di Microsoft Exchange Server o Lotus Domino, le cartelle pubbliche vengono create automaticamente a conclusione del processo di configurazione.

Per abilitare la scansione delle cartelle pubbliche, seguire le istruzioni nelle sezioni che seguono.

2.3.1 Configurazione della scansione di cartelle pubbliche per Microsoft Exchange Server

1. Dalla console di GFI MailEssentials configuration, fare clic con il pulsante destro del mouse sul nodo **Antispam ► Impostazioni antispam** e selezionare **Proprietà**.



Schermata 2 - Configurazione della scansione della cartella pubblica

2. Selezionare la scheda **Scansione della cartella pubblica** e fare clic sulla casella di controllo **Abilita scansione cartella pubblica**.

3. Dall'elenco **Eseguire il polling delle cartelle pubbliche tramite**, selezionare il metodo che GFI MailEssentials usa per recuperare i messaggi di posta elettronica dalle cartelle pubbliche.

- **Per Exchange Server 2000/2003,** selezionare MAPI, IMAP o WebDAV.
- **Per Exchange Server 2007,** scegliere WebDAV o Web Services.
- **Per Exchange Server 2010,** scegliere Web Services

Le opzioni disponibili sono:

- **MAPI:** per usare MAPI, GFI MailEssentials deve essere installato sul computer su cui è installato Microsoft Exchange Server. Non sono richieste altre impostazioni.
- **IMAP:** richiede il servizio Microsoft Exchange IMAP. IMAP consente la scansione remota delle cartelle pubbliche e opera bene negli ambienti che utilizzano firewall. Inoltre, IMAP può essere usato con altri server di posta che supportano IMAP. Parametri richiesti:
  - o nome del server di posta
  - o Numero della porta (la porta predefinita di IMAP è 143)

- Nome utente/password
- Selezionare l'opzione **Usa SSL** per una connessione sicura

- **WebDAV -** Specifica il nome del server di posta, la porta (la porta predefinita di WebDAV è 80), il nome utente/la password e il dominio. Selezionare la casella di controllo **Usa SSL** per una connessione sicura. Per impostazione predefinita, le cartelle pubbliche sono accessibili nella directory virtuale "public". Se questa è stata cambiata, specificare il nome corretto della directory virtuale per accedere alle cartelle pubbliche modificando il testo nella casella **URL**.
- **Web Services -** Specifica il nome del server di posta, la porta (la porta predefinita di Web Services è 80), il nome utente/la password e il dominio. Selezionare la casella di controllo **Usa SSL** per una connessione sicura. Per impostazione predefinita, le cartelle pubbliche sono accessibili nella directory virtuale "EWS/exchange.asmx". Se questa è stata cambiata, specificare il nome corretto della directory virtuale per accedere alle cartelle pubbliche modificando il testo nella casella **URL**.

Schermata 3 - Prova scansione della cartella pubblica riuscito

4. Fare clic su **Esegui scansione adesso** per creare automaticamente cartelle pubbliche.

5. Fare clic su **Prova** in caso di configurazione di IMAP, WebDAV o Web Services. La notifica visualizzata sullo schermo confermerà l'esito positivo/negativo della prova. Se la prova non è riuscita, verificare/aggiornare le credenziali ed eseguire nuovamente la prova.

2.3.2 Configurazione di un account utente dedicato per Exchange Server 2000/3

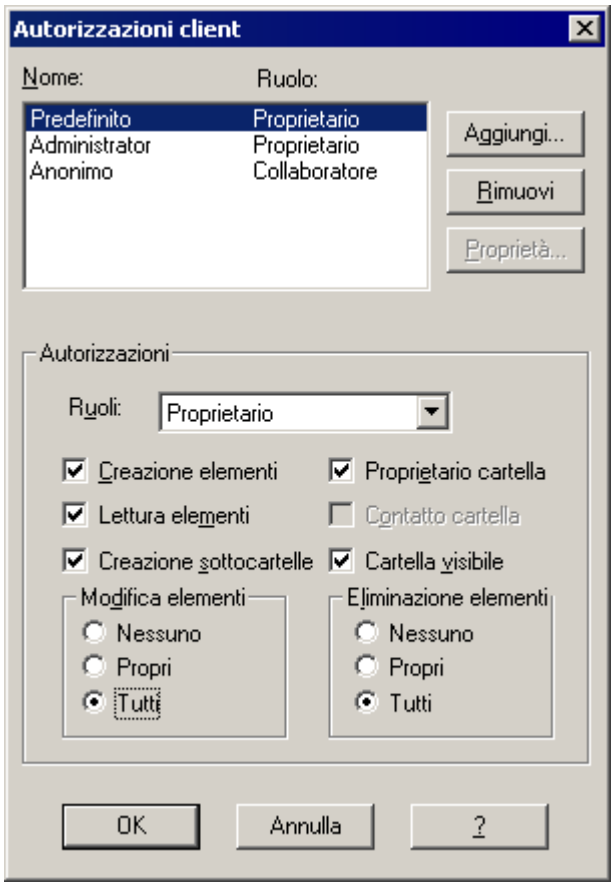
Se GFI MailEssentials viene installato in una DMZ, si raccomanda vivamente, per ragioni di sicurezza, di creare un account utente dedicato per recuperare/eseguire la scansione dei messaggi di posta elettronica presenti nelle cartelle pubbliche. Gli utenti avranno accesso a Cartelle anti-spam GFI.

1. Creare un nuovo utente di Active Directory (AD) con i privilegi dell'utente accreditato.

2. Da Microsoft Exchange System Manager, espandere **Cartelle** ► nodo **Cartelle pubbliche**.

3. Fare clic con il pulsante destro del mouse sulla cartella pubblica **Cartelle anti-spam GFI** e selezionare **Proprietà**.

4. Fare clic sulla scheda **Autorizzazioni** e selezionare **Autorizzazioni client**.



Schermata 4 - Impostazione del ruolo dell'utente.

5. Fare clic su **Aggiungi …**, selezionare nuovo utente e fare clic su **OK**.

6. Selezionare un nuovo utente dall'elenco delle autorizzazioni client e dall'elenco fornito impostare il suo ruolo su "Proprietario". Accertarsi che tutte le caselle di controllo siano selezionate e che i pulsanti radio siano impostati su **Tutti**.

7. Fare clic su **OK** per completare la configurazione.

8. Da Microsoft Exchange System Manager, fare clic con il pulsante destro del mouse su **Cartelle anti-spam GFI** e selezionare **Tutte le attività ► Diffusione impostazioni.**

NOTA: Per Microsoft Exchange Server 2003 SP2, fare clic su **Cartelle antispam GFI** e selezionare l'opzione **Tutte le attività ► Impostazioni di gestione**.

9. Selezionare l'opzione **Modifica autorizzazioni client** o **Diritti cartella** e fare clic su **OK** o **Avanti.**

10. Specificare le credenziali dell'account utente accreditato creato nella fase 1 ed eseguire la prova di configurazione per essere sicuri che le autorizzazioni siano corrette.

2.3.3 Configurazione di un account utente dedicato per Exchange Server 2007/2010

Alla configurazione di un account utente dedicato per recuperare i messaggi di posta elettronica dalle cartelle pubbliche antispam di GFI, l'utente dovrebbe avere i diritti di accesso del "proprietario" sulle

cartelle pubbliche antispam di GFI.

1. Creare un nuovo utente (accreditato) di Active Directory (AD).

2. Accedere a Microsoft Exchange Server usando i privilegi amministrativi.

3. Aprire “Microsoft Exchange Management Shell” e inserire il seguente comando:

```
Get-PublicFolder -Identity “\Cartelle anti-spam GFI” -Recurse | ForEach-Object {Add-PublicFolderClientPermission -Identity $_.Identity -User “USERNAME” -AccessRights owner -Server “SERVERNAME”}
```

4. Modificare “NOME UTENTE” e “NOME DEL SERVER” secondo i dettagli pertinenti all’utente dell’Active Directory in questione.

- Esempio:

```
Get-PublicFolder -Identity “\Cartelle anti-spam GFI” -Recurse | ForEach-Object {Add-PublicFolderClientPermission -Identity $_.Identity -User “mesuser” -AccessRights owner -Server “exch07”}
```

2.3.4 Come nascondere i messaggi dell’utente in Cartelle anti-spam GFI

Ai fini della riservatezza e sicurezza, si raccomanda vivamente di nascondere i messaggi creati su Cartelle anti-spam GFI. In questo modo, gli utenti potranno solamente inviare messaggi alle cartelle senza vedere i messaggi esistenti (compresi quelli inviati da loro stessi). Per configurare i privilegi dell’utente e nascondere i messaggi per gli utenti non autorizzati, procedere come descritto di seguito:

1. Da Microsoft Exchange System Manager, espandere **Cartelle** ► nodo **Cartelle pubbliche**.

2. Fare clic con il pulsante destro del mouse sulla cartella pubblica **Cartelle anti-spam GFI** e selezionare **Proprietà**.

3. Selezionare la scheda **Autorizzazioni** e fare clic su **Autorizzazioni client**.

4. Fare clic su **Aggiungi …**, selezionare l’utente/il gruppo a cui nascondere i messaggi e fare clic **OK**.

5. Selezionare l’utente/il gruppo configurato precedentemente nell’elenco delle autorizzazioni client e impostare il suo ruolo su **Contribuente**.

6. Accertarsi che sia selezionata solamente la casella di controllo **Crea elementi** e che i pulsanti radio siano impostati su **Nessuno**.

7. Fare clic su **OK** per completare la configurazione.

8. Da Microsoft Exchange System Manager, fare clic con il pulsante destro del mouse su **Cartelle anti-spam GFI** e selezionare **Tutte le attività ► Diffusione impostazioni.**

9. Selezionare la casella di controllo **Diritti cartella** e fare clic su **OK**.

2.3.5 Configurazione della scansione della cartella pubblica per i server Lotus Domino

Fase 1: Creare un nuovo data base per archiviare le cartelle pubbliche di GFI MailEssentials.

1. Da IBM Domino Administrator, fare clic su **File ► Data base ► Nuovo**.

2. Inserire le seguenti informazioni per il nuovo data base:

- Server: <*I dati del Domino Server dell'utente*>
- Titolo: Cartella pubblica
- Nome file: Public-F.nsf
- Selezionare "Mail (R7)" come modello per il nuovo data base

3. Fare clic su **OK** per creare il data base.

Fase 2: Convertire il formato del data base del data base appena creato.

1. Dalla console di Lotus Domino Server, eseguire il comando seguente:

```
Load Convert -e -h <Data base Filename>
```

- Esempio:

```
Load Convert -e -h Public-F.nsf
```

Fase 3: Creare un nuovo data base per la posta in arrivo:

È necessario creare una nuova cassetta postale per archiviare la nuova cartella pubblica di GFI MailEssentials.

1. Da IBM Domino Administrator, selezionare la scheda **Persone e Gruppi** e fare clic su **Data base posta in arrivo e Risorse**.

2. Fare clic su **Aggiungi data base posta in arrivo** e inserire il nuovo data base della posta in arrivo nel modo seguente:

- Nome posta in arrivo: Cartelle pubbliche
- Descrizione: Cassetta postale di GFI MailEssentials
- Indirizzo Internet: <*public@yourdomain.com*>
- Messaggio Internet: "Nessuna preferenza"
- Criptaggio posta in entrata: "No"
- Dominio: <*yourdomain*>
- Server: <*Your Domino server name*>
- Nome file: "Public-F.nsf"

NOTA: occorrerà associare un utente al data base della posta in arrivo creato. Questo account verrà usato dal server di GFI MailEssentials per connettersi al Lotus Domino Server.

Fase 4: Configurazione di GFI MailEssentials

Definire lo spazio dei nomi condiviso che verrà utilizzato durante la connessione con il servizio Lotus Domino IMAP:

1. Fare clic su **Start ► Esegui** e digitare **Regedit**.

2. Collocare la seguente chiave di registro:

```
<HKEY_LOCAL_MACHINE\SOFTWARE\GFI\ME14\Attendant\rpfolders:8\>
```

3. Creare le chiavi seguenti:

- Nome: “FolderDelimiter”
- Tipo: STRING
- Valore: ‘\\’

- Nome: “SharedNamespace”
- Tipo: STRING
- Valore: < Prefisso/Nome cartella pubblica del nuovo data base per la posta in arrivo \>

Ottenere i valori per la chiave “sharednamespace” nel modo seguente:

- **Nome del prefisso della cartella pubblica**

  1. Da IBM Domino Administrator, fare clic sulla scheda **Configurazione**.

  2. Espandere **Server ► Configurazioni,** fare clic sul proprio Domino Server e poi su **Modifica configurazione.**

  3. Dalla scheda **IMAP**, selezionare la scheda **Cartelle pubbliche e di altri utenti**. “Prefisso della cartella pubblica” si trova nella sezione Cartella pubblica.

- **Nome del data base per la posta in arrivo**

  1. Da IBM Domino Administrator, selezionare la scheda **Persone e Gruppi**.

  2. Fare clic sul nodo **Data base posta in arrivo e risorse**. Il nome del nuovo data base per la posta in arrivo è elencato nel pannello a destra.

Fase 5: Riavviare il servizio IMAP sul Domino Server

1. Aprire la console Lotus Notes

2. Scrivere “tell imap quit” e attendere fino al termine dell’attività.

3. Dopodiché, scrivere “load imap”

Fase 6: Configurazione di GFI MailEssentials

Configurare le proprietà di scansione della cartella pubblica di GFI MailEssentials.

1. Da GFI MailEssentials configuration, fare clic con il pulsante destro del mouse sul nodo **Antispam ► Impostazioni antispam** e selezionare **Proprietà**.

2. Selezionare la scheda **Scansione cartella pubblica** e inserire i valori seguenti:

- Server: <*Indirizzo IP del Domino Server*>
- Porta: 143 (impostazione predefinita)
- Nome utente: nome utente associato al data base della posta in arrivo
- Password: password dell’utente

3. Eseguire la prova della configurazione facendo clic sul pulsante **Prova** e su **Esegui scansione adesso** per generare le cartelle pubbliche.

Fase 7: Accertarsi che le cartelle pubbliche siano state create

Usare Telnet per stabilire se le cartelle pubbliche sono state create con successo:

1. Dalla finestra di comando per il caricamento del computer di GFI MailEssentials.

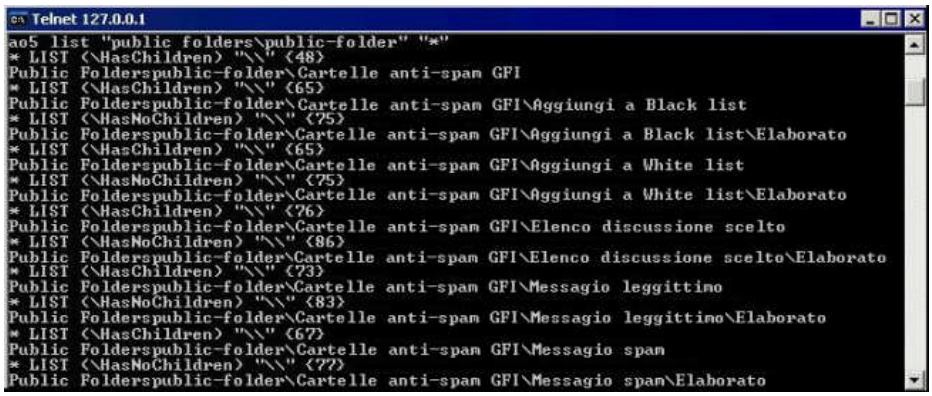
2. Scrivere “telnet”

3. Scrivere “Open <*INDIRIZZO IP*> 143”

4. Scrivere “ao1 login <public@yourdomain.com> <password>“

5. Scrivere “ao5 list “<Prefisso/Nome cartella pubblica del nuovo data base per la posta in arrivo\>“ “*”

6. L’esito del comando di cui sopra dovrebbe mostrare le cartelle pubbliche come nella schermata in basso:



7. Scrivere “ao3 logout”

NOTA: usare il designer di Lotus Notes per eliminare visualizzazioni e forme non desiderate dal data base creato precedentemente.

3 Amministrazione di routine

3.1 Revisione dei messaggi di spam

3.1.1 Procedura per la revisione dello spam

1. Invitare i singoli utenti della posta elettronica a revisionare periodicamente i messaggi di spam.

2. Nel caso in cui alcuni messaggi di posta elettronica legittimi venissero individuati come spam, fare riferimento alla sezione Gestione dei messaggi di posta elettronica legittimi in basso per ordinare a GFI MailEssentials di non classificare messaggi di posta elettronica simili come spam.

3. Nel caso in cui alcuni messaggi di spam venissero erroneamente individuati come spam (falsi positivi), fare riferimento alla sezione Gestione dello spam in basso per consultare le istruzioni di GFI MailEssentials sulla classificazione dei messaggi di posta elettronica simili come spam.

3.2 Gestione dei messaggi di posta elettronica legittimi

Come avviene con qualsiasi soluzione antispam, GFI MailEssentials potrebbe richiedere un po' di tempo prima che possano essere raggiunte le condizioni di filtraggio antispam ottimali. Se questo obiettivo non viene conseguito, potrebbe darsi che alcuni messaggi di posta elettronica legittimi siano stati individuati come spam.

In questi casi, gli utenti dovrebbero aggiungere i messaggi di posta elettronica erroneamente individuati come spam ad "Aggiungi a White list" e alle cartelle "**Messaggio legittimo**" per "insegnare" a GFI MailEssentials che il messaggio in questione non è uno spam.

Note importanti

In Microsoft Outlook, è possibile trascinare e posizionare il messaggio di posta elettronica nell'apposita cartella selezionata. Per mantenere una copia del messaggio di posta elettronica, premere il tasto **CTRL** per copiare il messaggio anziché spostarlo.

3.2.1 Aggiunta di mittenti o newsletter alla white list

1. Nelle cartelle pubbliche, individuare la cartella pubblica **Cartelle anti-spam GFI ► Aggiungi a White list**

2. Trascinare e lasciare i messaggi di posta elettronica o le newsletter nella cartella pubblica **Aggiungi a White list.**

3.2.2 Aggiunta di liste di discussione alla white list

Spesso vengono inviate liste di discussione **(NON newsletter)** che non includono l'indirizzo di posta elettronica del destinatario nel campo "*MIME TO* (MIME A)" e perciò sono contrassegnate come spam. Se si desidera ricevere tali liste di discussione, è necessario inserire nella white list gli indirizzi di posta elettronica dei mailer di tali liste legittime.

Come aggiungere liste di discussione alla white list

1. Nelle cartelle pubbliche, individuare la cartella pubblica **Cartelle anti-spam GFI ► Elenco discussione scelto.**

2. Trascinare e lasciare le liste di discussione nella cartella pubblica **Elenco discussione scelto**.

3.2.3 Aggiunta di ham al data base dei messaggi posta elettronica legittimi

1. Nelle cartelle pubbliche, individuare la cartella pubblica **Cartelle anti-spam GFI ► Messaggio legittimo.**

2. Trascinare e lasciare i messaggi di posta elettronica nella cartella pubblica **Messaggio legittimo.**

3.3 Gestione dello spam

Anche se GFI MailEssentials inizia a individuare i messaggi di spam dalla cassetta, potrebbero presentarsi casi in cui lo spam riesce a passare inosservato nella cassetta postale dell'utente. In genere, ciò potrebbe essere dovuto alle impostazioni della configurazione non ancora eseguite o a nuove forme di spam a cui GFI MailEssentials non si è ancora adattato. In entrambi i casi, tali situazioni vengono risolte quando GFI MailEssentials è configurato per catturare tali spam.

NOTA: per maggiori informazioni sulla modalità di risoluzione dei problemi legati ai messaggi di posta elettronica non rilevati come spam, consultare il capitolo Risoluzione dei problemi e assistenza a pagina 128 del presente manuale.

In questi casi, gli utenti dovrebbero aggiungere tali messaggi di posta elettronica ad "Aggiungi a Black list" e alle cartelle "Questo è un messaggio di spam" per "insegnare" a GFI MailEssentials che il messaggio in questione è uno spam.

Note importanti

1. In Microsoft Outlook, è possibile trascinare e posizionare il messaggio di posta elettronica nell'apposita cartella selezionata. Per mantenere una copia del messaggio di posta elettronica, premere il tasto **CTRL** per copiare il messaggio anziché spostarlo.

2. Consultare la sezione Abilitazione della scansione della cartella pubblica a pagina 9 del presente manuale per maggiori informazioni sulla modalità di creazione automatica di **Cartelle anti-spam GFI**.

3.3.1 Aggiunta di mittenti alla black list

1. Nelle cartelle pubbliche, individuare la cartella pubblica **Cartelle anti-spam GFI ► Aggiungi a Black list.**

2. Trascinare e lasciare i messaggi di posta elettronica nella cartella pubblica **Aggiungi a Black list.**

3.3.2 Aggiunta di spam al data base spam

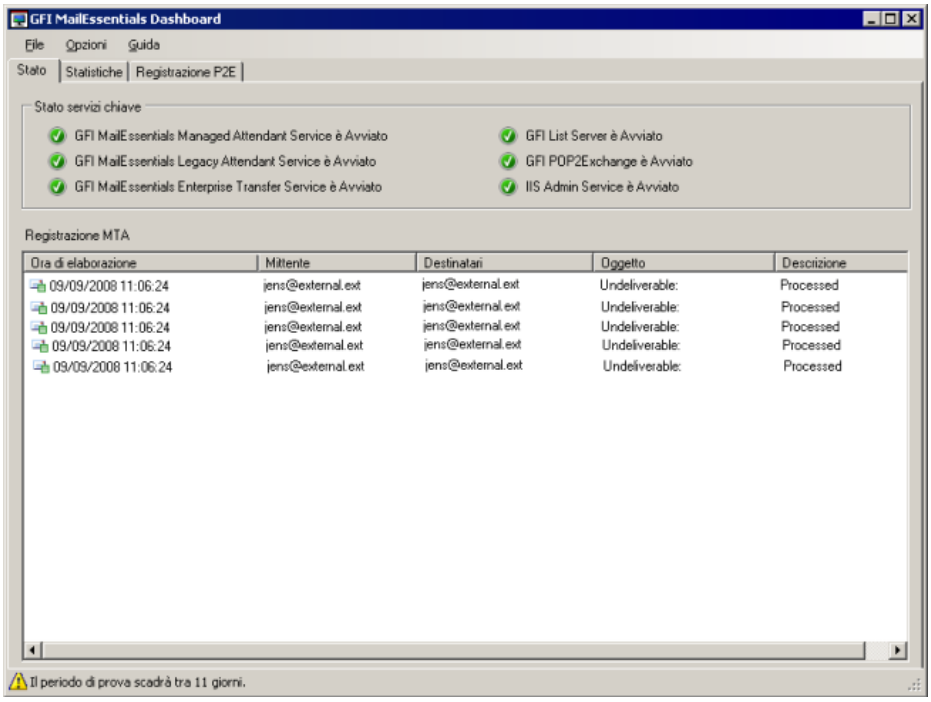
1. Nelle cartelle pubbliche, individuare la cartella pubblica **Cartelle anti-spam GFI ► Questo è un messaggio di spam.**

2. Trascinare e lasciare il messaggio di spam nella cartella pubblica **Messaggio spam**.

3.4 Visualizzazione dello stato antispam sulla dashboard

GFI MailEssentials dashboard mostra lo stato del sistema antispam, oltre all'attività di elaborazione della posta elettronica e le statistiche. Utilizzare GFI MailEssentials dashboard come indicato qui di seguito:

1. Fare clic su **Start ► Tutti i programmi ► GFI MailEssentials ► GFI MailEssentials Dashboard**.



Schermata 5 -GFI MailEssentials Dashboard

2. Fare clic su:

- **Stato** per visualizzare lo stato dei servizi e l'attività di elaborazione dei messaggi di posta elettronica di GFI MailEssentials.
- **Statistiche** per visualizzare i grafici dei dati statistici indicanti il flusso dei messaggi di posta elettronica e lo spam bloccato da tutti i filtri antispam, nonché i contatori recanti le informazioni sui messaggi di posta elettronica e sullo spam in entrata e in uscita.
- **P2E Logging:**mostra un registro delle attività di POP2Exchange.

NOTA: per maggiori informazioni su POP2Exchange, consultare la sezione Configurazione dello scaricamento POP3 a pagina 99 del presente manuale.

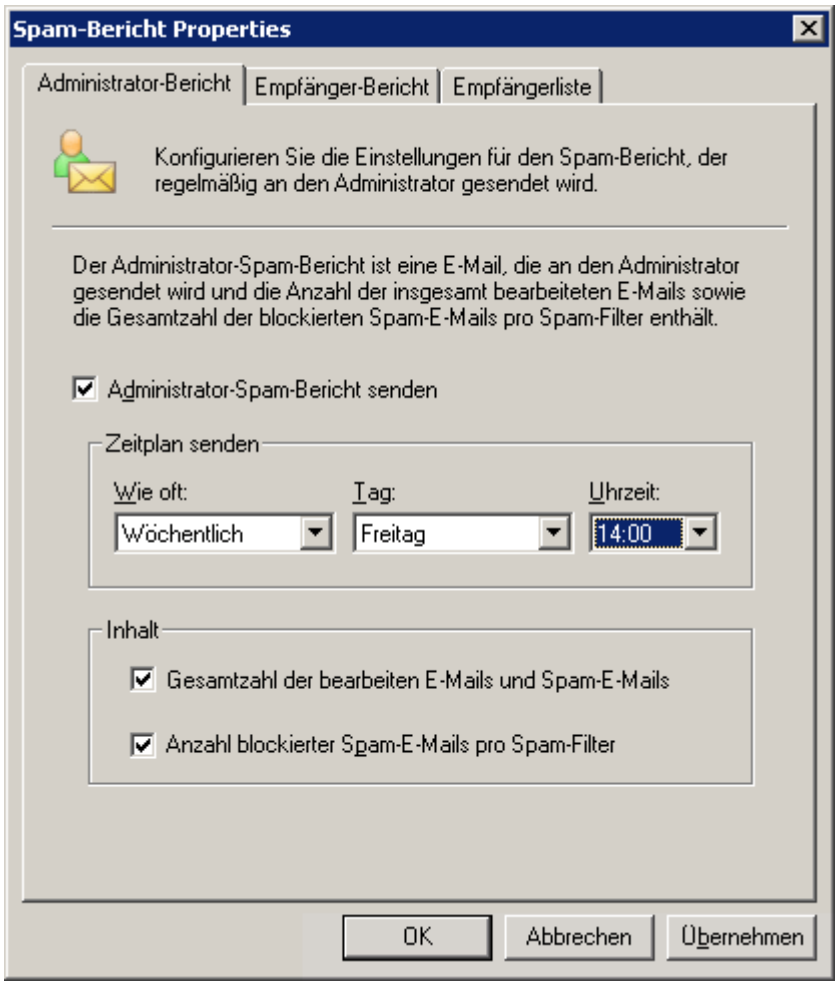
3.5 Creazione di raccolta di spam (Spam Digest)

Il Spam Digest è un breve rapporto inviato a un amministratore o utente mediante posta elettronica. Questo rapporto elenca il numero complessivo di messaggi di posta elettronica elaborati da GFI MailEssentials e il numero di messaggi di spam bloccati nell'arco di un periodo di tempo specifico (essenzialmente dall'ultima raccolta di spam).

3.5.1 Configurazione del Spam Digest

Raccolta di spam per l'amministratore

1. Selezionare **Antispam ► Spam Digest ► Proprietà.**



Schermata 6 - Proprietà del Spam Digest dell'amministratore

2. Dalla scheda **Raccolta amministratore**, fare clic su **Invia raccolta di spam all'amministratore** per abilitare la raccolta di spam.

3. Configurare la frequenza di invio desiderata (giornaliera, settimanale, mensile) dalla lista a cascata **Calendario di invio**.

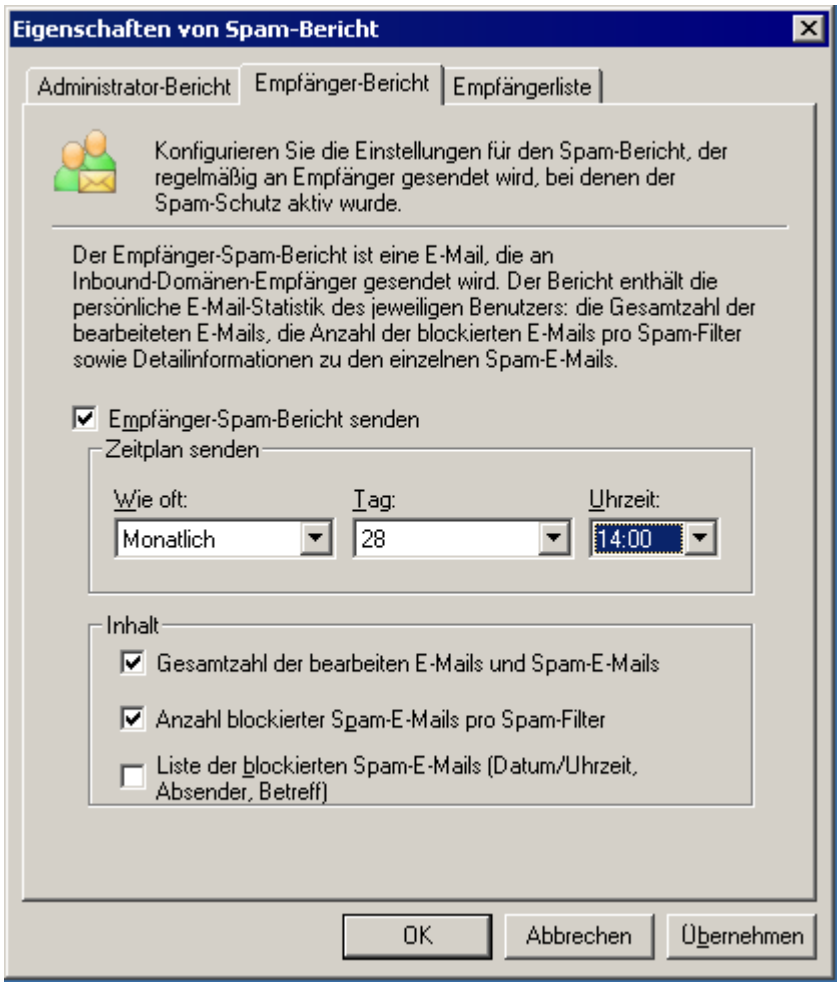
4. Specificare il contenuto della raccolta che verrà inviato nel

messaggio di posta elettronica: Conteggio **complessivo di messaggi di posta elettronica e spam elaborati** o **Spam complessivi catturati per filtro antispam** o entrambi.

5. Completare le impostazioni selezionando **Applica** e **OK**.

Raccolta di spam per il destinatario

1. Selezionare **Antispam ► Raccolta di spam ►Proprietà.**



Schermata 7 - Raccolta di spam per il destinatario

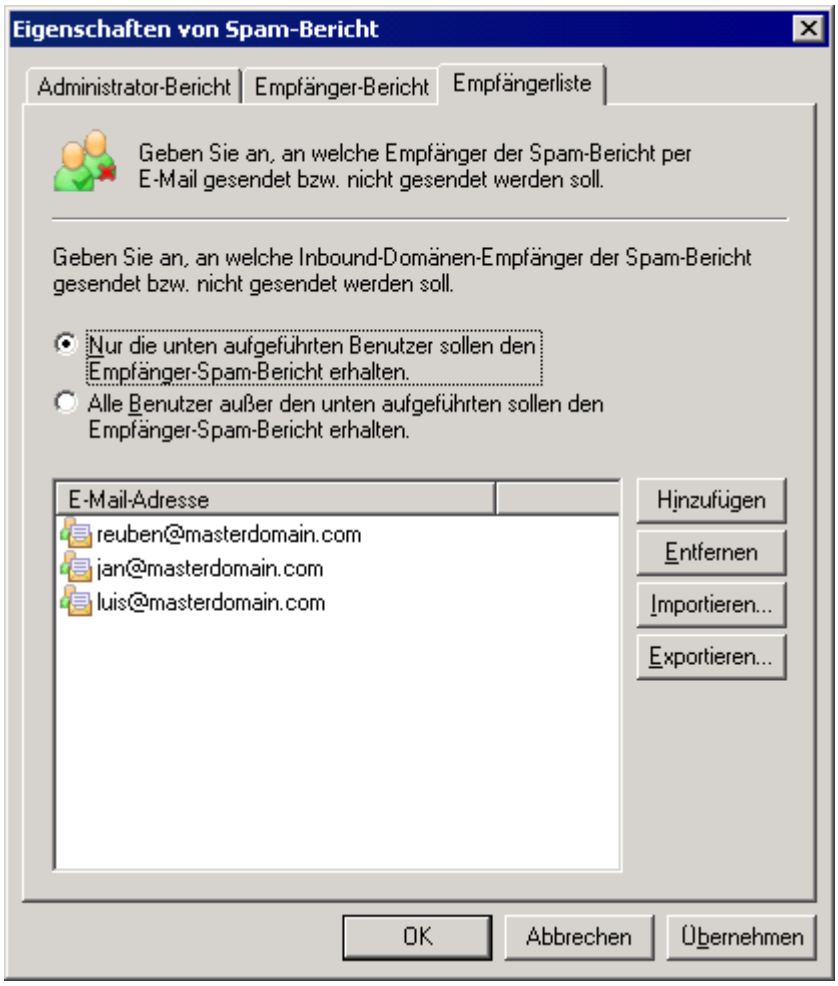
2. Dalla scheda **Raccolta destinatario**, selezionare **Invia raccolta di spam al destinatario** per abilitare la raccolta di spam.

3. Configurare la frequenza di invio desiderata dal **Calendario di invio**.

4. Specificare il contenuto della raccolta che verrà inviato nel messaggio di posta elettronica:

- conteggio complessivo di messaggi di posta elettronica e spam elaborati
- spam complessivi catturati per filtro antispam
- lista di spam bloccati

o eventualmente qualsiasi combinazione delle opzioni.



Schermata 8 - Lista dei destinatari a cui inviare la raccolta di spam

5. Fare clic sulla scheda **Lista destinatari**, aggiungere gli utenti a cui inviare la raccolta di spam e selezionare il metodo per stabilire chi dovrebbe ricevere la raccolta di spam. Le opzioni disponibili sono:

- solamente gli utenti sotto elencati dovrebbero ricevere la raccolta di spam;
- tutti gli utenti, tranne quelli sotto elencati riceveranno la raccolta di spam.

NOTA: la lista degli utenti richiesta può anche essere importata da un file in formato XML nella medesima struttura con cui GFI MailEssentials esporterebbe i file.

6. Selezionare **Applica** e **OK** per completare le impostazioni.

3.6 Creazione di archivi per la posta elettronica

GFI MailEssentials consente di utilizzare la funzione di archiviazione con cui mantenere i registri cronologici di tutte le comunicazioni dell'utente via posta elettronica. Dal momento che GFI MailEssentials è una soluzione antispam, la funzione di archiviazione integrata non è intesa a sostituire/replicare la funzionalità fornita dalla soluzione di archiviazione della posta elettronica di GFI MailArchiver.

L'archiviazione richiede una tecnologia basata su data base. GFI MailEssentials supporta sia Microsoft Access sia Microsoft SQL

Server.

Note importanti

1. I messaggi di posta elettronica interni non vengono archiviati.

2. Per reti più estese, si consiglia Microsoft SQL Server.

3. L'uso di Microsoft Access limita le dimensioni del data base a 2 GB. MSDE e SQL Server Express sono limitati a 2 e 4 GB, rispettivamente.

4. Quando un data base Microsoft Access raggiunge 1GB un messaggio di posta elettronica viene inviato all'amministratore consigliando di passare a un server Microsoft SQL.

3.6.1 Come abilitare l'archiviazione

1. Dalla console di GFI MailEssentials configuration fare clic con il pulsante destro del mouse su **Gestione posta elettronica ► Archiviazione della posta** e selezionare **Proprietà**.

2. Fare clic su **Archiviazione della posta** e selezionare se archiviare i messaggi di posta elettronica in arrivo e/o in uscita.

3. Selezionare e configurare il metodo di archiviazione:

- **Archivia i messaggi di posta elettronica in un file di testo** - Archivia i messaggi di posta elettronica in arrivo e in uscita in file di testo in arrivo e in uscita separati. Gli allegati dei messaggi di posta elettronica non vengono archiviati se si seleziona questa opzione.
- **Archivia i messaggi di posta elettronica in un data base** - Archivia tutti i messaggi di posta elettronica in un data base di Microsoft Access o SQL/SQL Server Express/MSDE. Questa funzione consente l'archiviazione degli allegati ai messaggi di posta elettronica.

4. Per escludere l'archiviazione di messaggi di posta elettronica provenienti da taluni utenti, selezionare la scheda **Eccezioni,** spuntare **Non archiviare i messaggi di posta elettronica in cui il mittente o il destinatario risulta nell'elenco in basso,** fare clic sul pulsante **Aggiungi** e aggiungere l'indirizzo di posta elettronica dell'utente nell'elenco di **Posta elettronica**.

5. Fare clic con il pulsante **OK** per completare la configurazione.

3.6.2 Abilitazione per l'accesso a Archive Web Interface da GFI MailEssentials

Note importanti

1. GFI MailEssentials Archive Web Interface non è supportata sui sistemi operativi 64 bit.

Installazione di GFI MailEssentials Archive Web Interface (AWI) su Microsoft IIS 7.0 (sistemi x86)

Per installare AWI su Microsoft IIS 7.0, è necessario:

- installare IIS Web Server Role Services;
- configurare l'applicazione Web di IIS che sarà usata da AWI.

AWI richiede i seguenti IIS Web Server Role Services per funzionare correttamente:

- ASP
- Autenticazione Windows

Per installare IIS Web Server Role Services su Microsoft Windows 2008:

1. aprire il “Server Manager”;

2. espandere il nodo **Ruoli** e selezionare **Server Web (IIS)**;

3. dal pannello a destra, fare clic con il pulsante **Aggiungi servizi ruolo**;

4. selezionare i servizi ruolo “ASP” e “Autenticazione di Windows” e fare clic su **Avanti;**

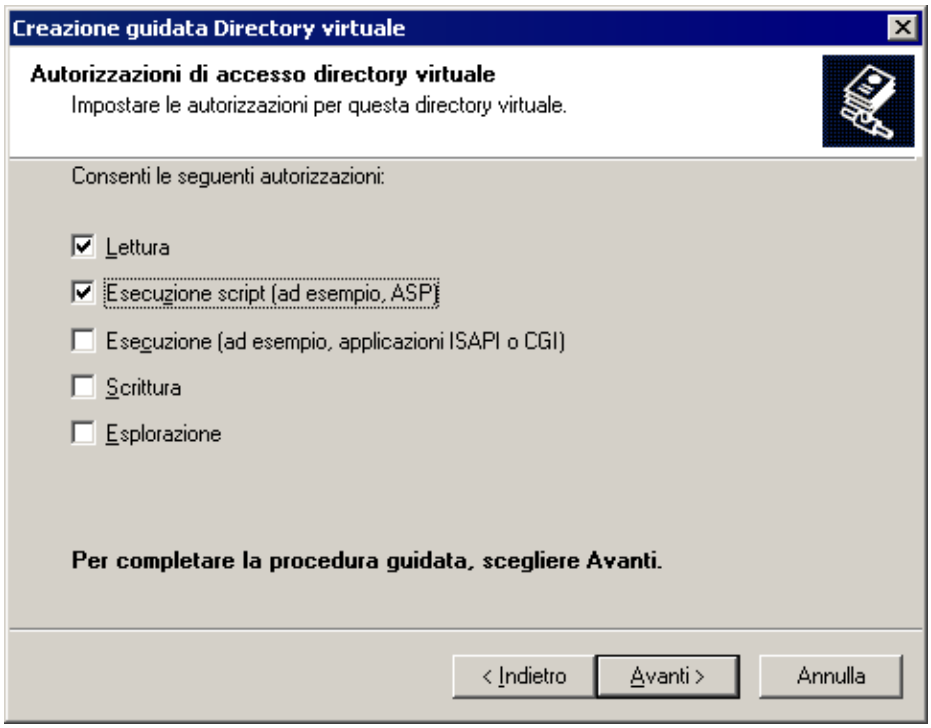
5. fare clic con il pulsante **Installa** per installare i servizi ruolo.

Configurare l’applicazione Web di IIS che sarà usata da AWI su IIS 6.0

1. Avviare Internet Services Manager Gestione servizio Internet, fare clic con il pulsante destro del mouse sul nodo del sito Web e dal menu a comparsa selezionare **Nuova ► Directory virtuale**. Viene visualizzata la **Procedura guidata Creazione directory virtuale.** Fare clic su **Avanti** per continuare.

2. Si deve ora inserire un alias per la directory virtuale. In questo caso si tratta di AWI, ma è possibile immettere qualsiasi nome, purché rispetti le convenzioni sulla denominazione di cartelle utilizzate in Microsoft Windows.

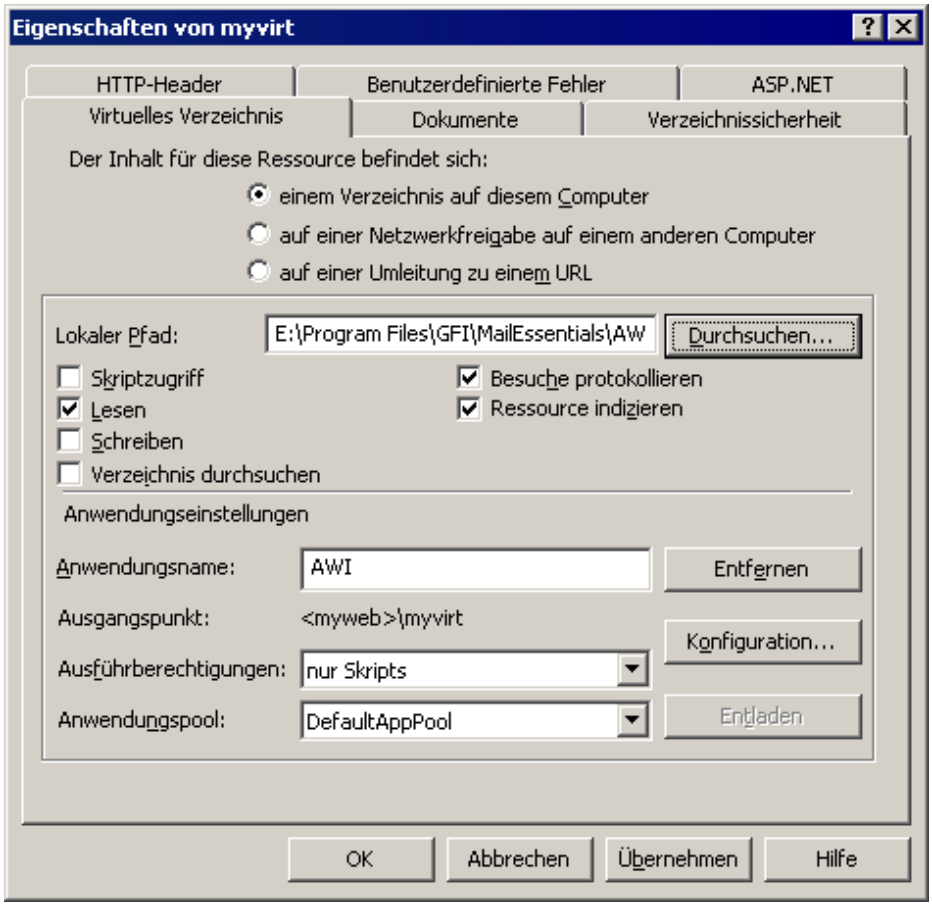
3. È necessario quindi inserire il percorso in cui è localizzato il contenuto. Fare clic con il pulsante **Sfoglia** e selezionare la cartella “AWI\wwwroot” nel percorso d’installazione di GFI MailEssentials.



Schermata 9 - Impostazione delle autorizzazioni

4. Si devono poi impostare le autorizzazioni di accesso. Selezionare unicamente le caselle di controllo **Leggi** ed **Esegui script (quali ASP)**. Accertarsi che tutte le altre caselle di controllo siano deselezionate. Fare clic con il pulsante **Avanti** e, sulla pagina finale, fare clic con il pulsante **Fine** per terminare la Procedura guidata Creazione directory virtuale.

5. Fare clic con il pulsante destro del mouse sulla directory virtuale appena creata, situata sotto la root Web del server del proprio sito Web e selezionare **Proprietà** dal menu di scelta rapida.



Schermata 10 - Impostazione delle proprietà della Directory virtuale

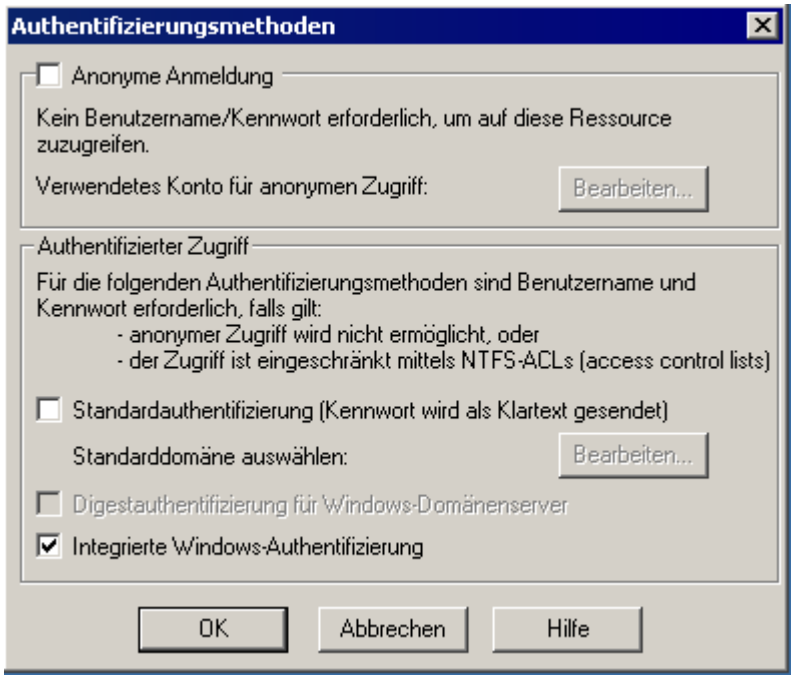
6. Nella scheda **Directory virtuale** della finestra di dialogo delle **Proprietà**, selezionare le caselle di controllo **Lettura**, **Registrazione visite** e **Indicizza questa risorsa**. Accertarsi che tutte le altre caselle di controllo siano deselezionate. Nella casella dell'elenco **Autorizzazioni di esecuzione**, selezionare **Solo script**.

7. Accedere alla scheda **Documenti**. Rimuovere tutti documenti predefiniti tranne **default.asp**.

8. Accedere alla scheda **Protezione directory** e fare clic con il pulsante **Modifica** situato nel gruppo **Controllo autenticazione e accesso**.

NOTA: poiché l'Interfaccia di archiviazione Web fornisce l'accesso a tutti i messaggi di posta elettronica archiviati da GFI MailEssentials, è importante configurare un'adeguata autenticazione e protezione per questo server Web e per la directory virtuale. Esistono tre modi per proteggere l'interfaccia di ricerca. Si tratta dell'autenticazione di base, digest e Windows integrata. L'Autenticazione Windows integrata

rappresenta la scelta preferita in un ambiente di Active Directory, perché rende uniforme il processo di autenticazione, non richiedendo inizialmente all'utente informazioni sul proprio nome utente o password. Adopera piuttosto le informazioni utente di Windows correnti, presenti sul computer client per l'autenticazione. Se si sta installando GFI MailEssentials in una DMZ, si deve utilizzare l'autenticazione di base.



Schermata 11 - Selezionare il metodo di autenticazione

9. Selezionare la casella di controllo **Autenticazione Windows integrata**, consigliata se il prodotto è installato sulla rete interna, OPPURE **Autenticazione di base**, se è installato nella DMZ. Accertarsi che la casella di controllo **Abilita accesso anonimo** risulti deselezionata.

NOTA 1: se si utilizza l'Autenticazione Windows integrata, si verificherà un'autenticazione rispetto ad Active Directory. Pertanto, non sarà necessario configurare utenti aggiuntivi. Se si utilizza l'Autenticazione di base, l'autenticazione avviene rispetto al data base utenti locale presente sul computer. In tal caso, si devono creare nomi utente e password sul computer locale. Per maggiori informazioni sulla protezione di IIS, consultarne la relativa documentazione.

NOTA 2: **accertarsi che NON sia consentito l'accesso anonimo.**

10. Fare clic su **OK** per completare la configurazione.

Configurare l'applicazione Web di IIS che sarà usata da AWI su IIS 7,0

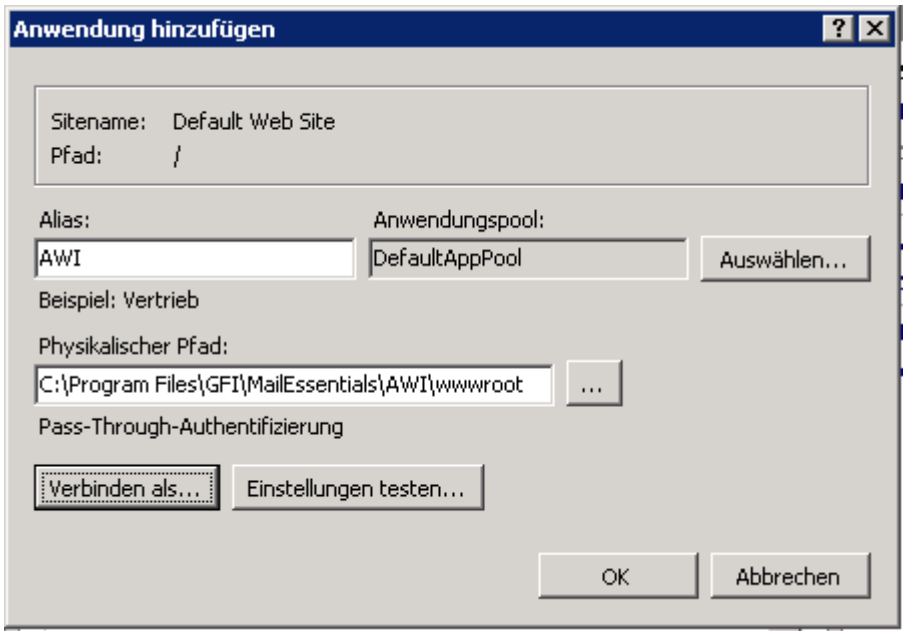
Per configurare AWI su IIS 7.0:

1. aprire "Strumenti amministrativi";

2. inserire "Internet Information Services (IIS) Manager";

3. fare clic con il pulsante destro del mouse sul sito Web che ospiterà l'interfaccia Web AWI e fare clic su **Aggiungi applicazione**.

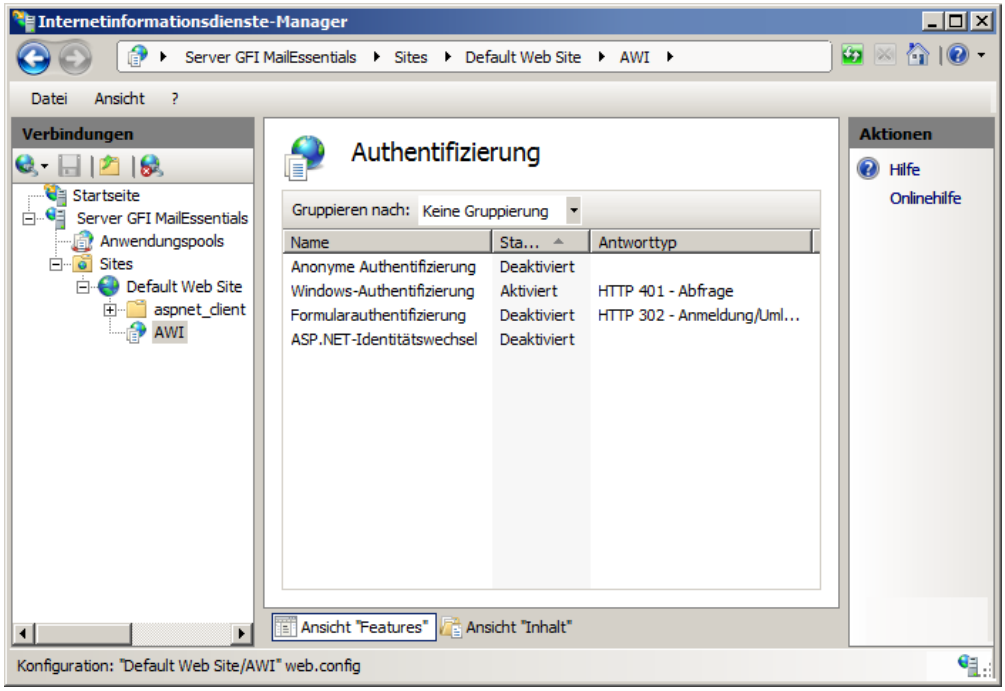
4. Immettere “AWI” come alias e inserire il percorso della cartella “wwwroot” AWI situata in <GFI\MailEssentials\AWI\wwwroot>.



Schermata 12 - Internet Information Services (IIS) Manager: Aggiungere applicazione

5. Fare clic su **OK** per creare la nuova applicazione.

6. Fare clic sull’applicazione “AWI” appena creata e fare doppio clic sull’icona **Autenticazione** nel pannello a destra.



Schermata 13 - Internet Information Services (IIS) Manager:

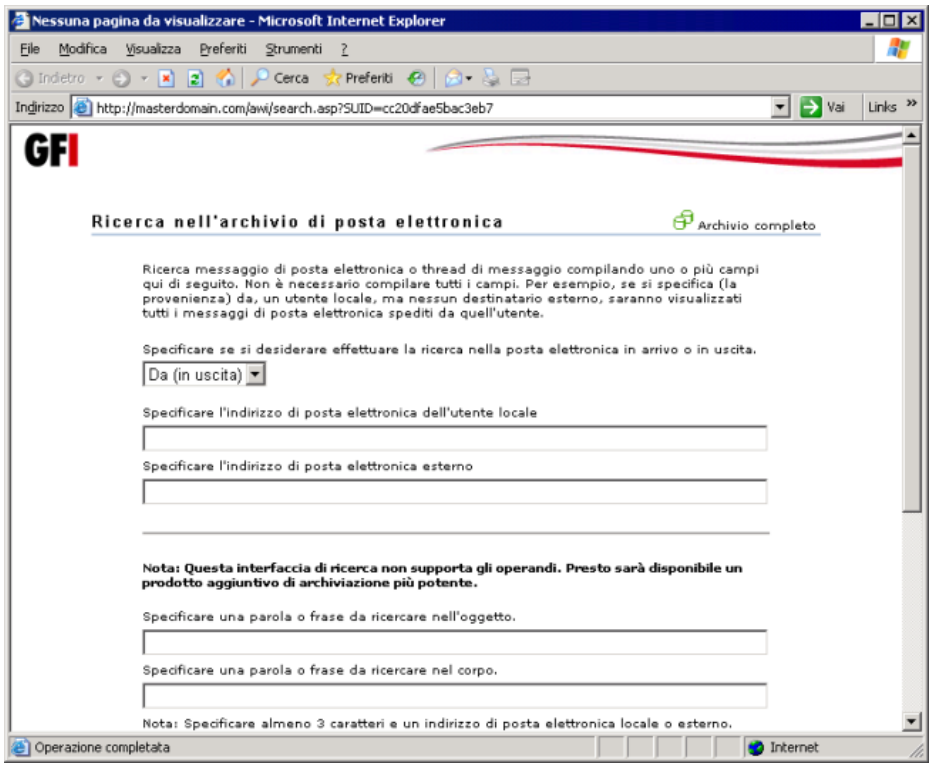
7. Fare clic con il pulsante destro del mouse sull’opzione **Autenticazione anonima** e selezionare **Disabilita**.

8. Fare clic con il pulsante destro del mouse sull’opzione **Autenticazione Windows** e selezionare **Abilita**.

3.6.3 Accesso a Archive Web Interface

1. Eseguire Internet Explorer.
2. Inserire: *http://<machine_name>/<awi_virtual_folder_name>*.

- **Esempio:** http://master-domain.com/awi/



Schermata 14 - Pagina di ricerca di Archive Web Interface(AWI)

L'AWI caricherà la pagina di ricerca. Fare clic sul link **Archivio completo** nell'angolo in alto a destra per accedere alla pagina di archivio completo.

3.7 Rapporti sulla situazione dello spam e sull'elaborazione dei messaggi di posta elettronica

GFI MailEssentials consente di generare rapporti sulla base dei dati archiviati nel data base. Questi rapporti informano l'utente sullo spam filtrato da GFI MailEssentials, sui livelli d'uso del server di posta e sulle risorse del dominio.

Note importanti

Abilitare l'archiviazione di GFI MailEssentials a usare i rapporti. Consultare la sezione Uso dei rapporti a pagina 31 del presente manuale per i dettagli sulla modalità di abilitazione dell'archiviazione.

3.7.1 Abilitazione dei rapporti

1. Selezionare **Gestione posta elettronica ► Gestione Report ► Proprietà** e fare clic con il pulsante **Configura.**
2. Selezionare il tipo di data base:

- **Microsoft Access** - Specificare il nome e la posizione del file.
- **Microsoft SQL server** - Specificare il nome del server, le credenziali di accesso e il data base.

3. Fare clic sul pulsante **Prova** per completare la configurazione del data base. Fare clic su **OK** per salvare le impostazioni.

3.7.2 Uso dei rapporti

1. Eseguire GFI MailEssentials Reporter facendo clic su **Start ► Tutti i programmi ► GFI MailEssentials ► GFI MailEssentials Reports.**

2. Fare clic sull'opzione **Rapporti** e selezionare l'opzione Rapporto o Statistiche.

3. Selezionare l'opzione dal menu **File ► Stampa** per stampare i rapporti.

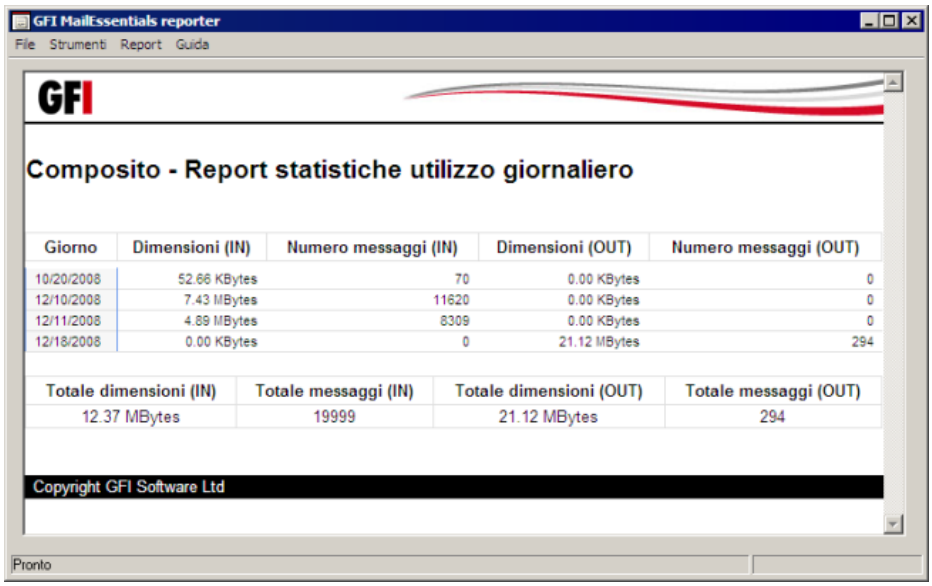
NOTA: selezionare **File ► Anteprima di stampa** per vedere come verrà stampato il rapporto.

4. Per salvare un rapporto, fare clic su **File ► Salva con nome**. Specificare un nome e una posizione per il file salvato, dopodiché fare clic sul pulsante **Salva**.

NOTA: il rapporto viene salvato nella posizione scelta con il nome specificato per il rapporto. Nella cartella specificata, vengono create due sottocartelle, "grafici" e "rapporto". La sottocartella "rapporto" contiene i file del rapporto in formato HTML. La sottocartella "grafici" contiene i grafici visualizzati nel rapporto in formato HTML.

Rapporto sullo spam giornaliero

Il rapporto sullo spam giornaliero mostra il numero totale di messaggi di posta elettronica elaborati, il numero totale di messaggi spam individuati, la percentuale di spam rispetto al totale di messaggi di posta elettronica elaborati e il numero di messaggi di spam individuati da ciascuna caratteristica antispam. Ciascuna riga del rapporto rappresenta un giorno.



Schermata 15 - Rapporto sullo spam giornaliero

Opzioni del rapporto

- **Ordina colonna:** ordina il rapporto per data, totale spam elaborato, controllo parola chiave, ecc.
- **Rapporto multi pagine:** permette di specificare il numero di giorni che si desidera visualizzare su ogni pagina.

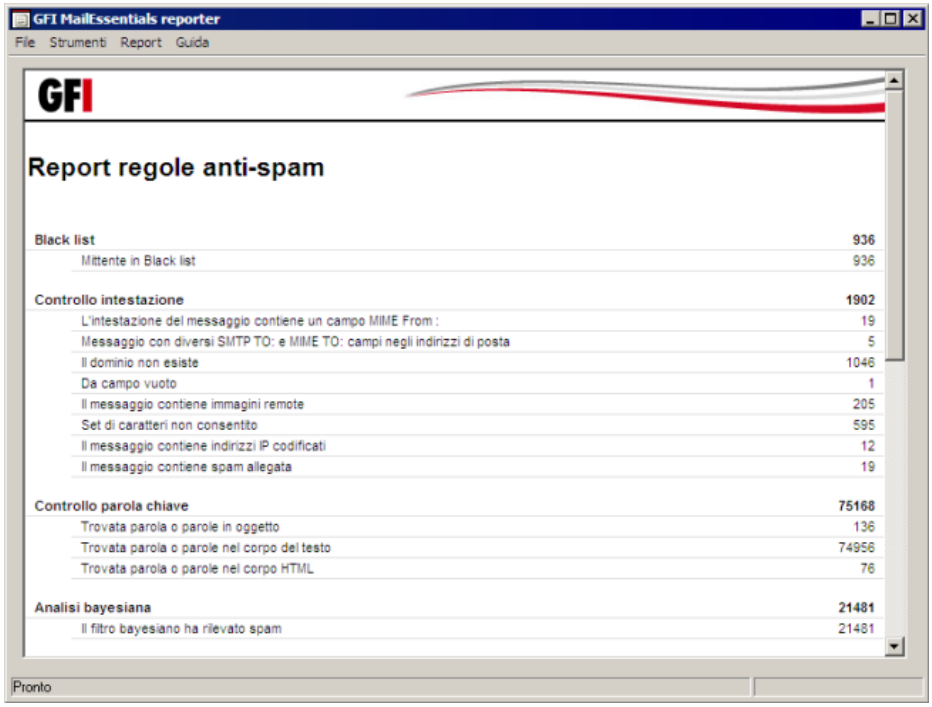
Opzioni di filtro

- **Indirizzo di posta elettronica specifico:** questa opzione limita il rapporto a un indirizzo di posta elettronica determinato.
- **Intervallo di date:** questa opzione limita il rapporto a un intervallo di date determinato.

Una volta selezionate le opzioni del rapporto, fare clic sul pulsante **Rapporto** per generare il rapporto.

Rapporto sulle Regole Antispam

Il Rapporto sulle Regole Antispam mostra la quantità di messaggi di spam rilevata da ciascun metodo.



Schermata 16 - Rapporto sulle Regole Antispam

Opzioni del rapporto

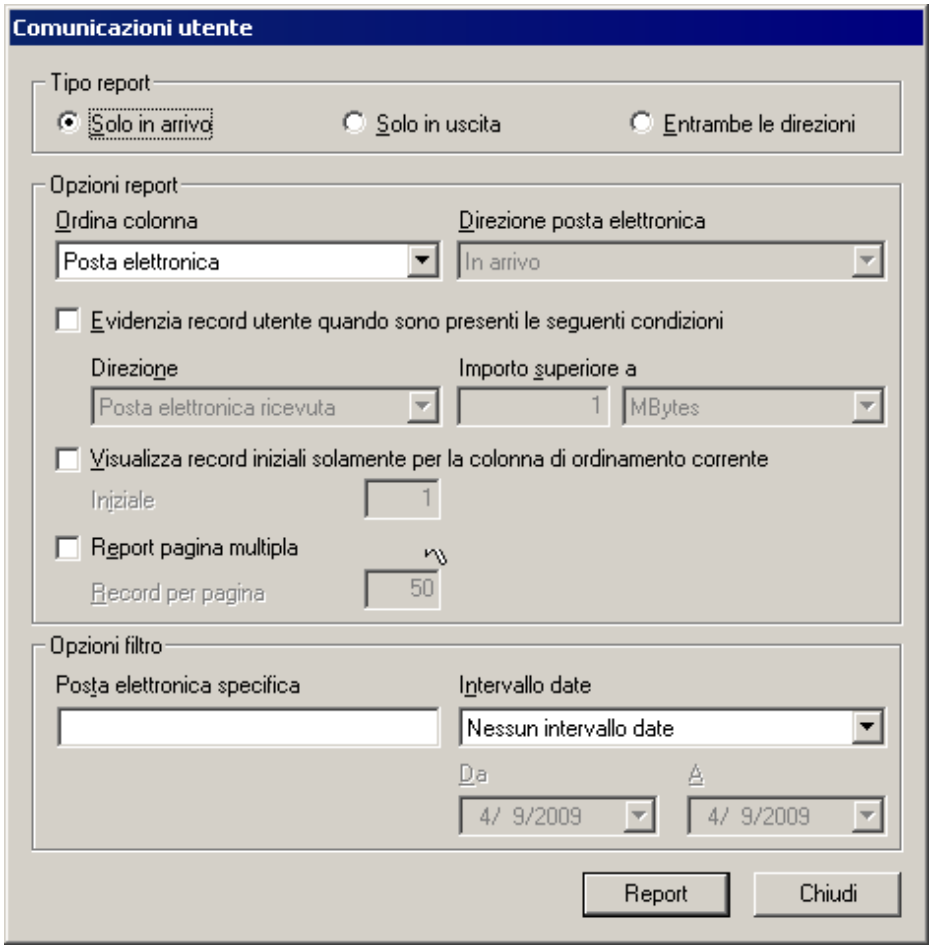
- **Indirizzo di posta elettronica specifico:** questa opzione limita il rapporto a un indirizzo di posta elettronica determinato.
- **Intervallo di date:** questa opzione limita il rapporto a un intervallo di date determinato.

Una volta selezionate le opzioni del rapporto, fare clic sul pulsante **Rapporto** per generare il rapporto.

Statistiche di utilizzo dell'utente

Il rapporto sulle statistiche di utilizzo dell'utente offre una panoramica sulla quantità e sulla dimensione dei messaggi di posta elettronica

inviati o ricevuti dagli utenti.



Schermata 17 - Finestra di dialogo del filtro per le statistiche di utilizzo dell'utente

Tipo di rapporto

- **Tipo di rapporto:** permette di indicare se si desidera generare un rapporto sui messaggi di posta elettronica in arrivo, in uscita o su entrambi.

Opzioni del rapporto

- **Ordina per:** consente di specificare se il rapporto deve essere ordinato per indirizzo di posta elettronica, numero di messaggi di posta elettronica o dimensione totale dei messaggi di posta elettronica.
- **Utenti selezionati:** consente di mettere in evidenza gli utenti che inviano o ricevono più di un determinato numero di messaggi di posta elettronica o di una determinata quantità di megabyte di messaggi di posta elettronica.
- **Inizio elenco:** permette di elencare soltanto i primi utenti del rapporto.
- **Rapporto multi pagine:** permette di specificare il numero di utenti che si desidera visualizzare su ogni pagina.

Opzioni di filtro

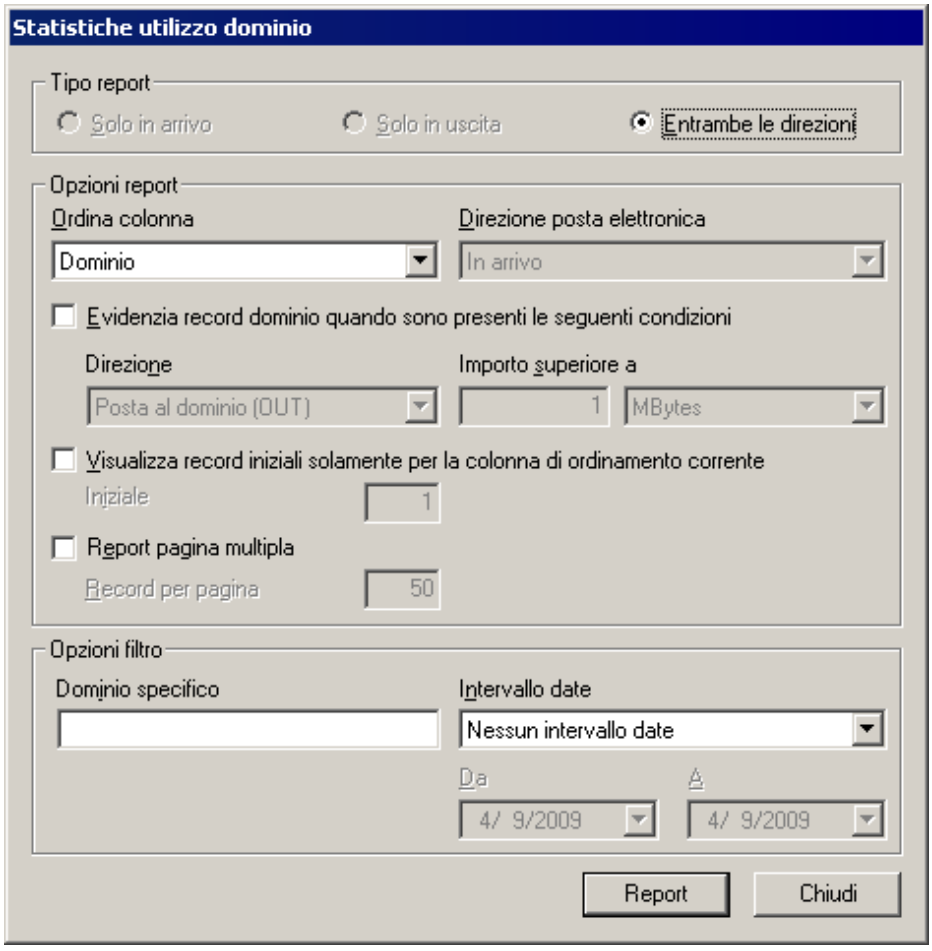
- **Indirizzo di posta elettronica specifico:** questa opzione limita il rapporto a un indirizzo di posta elettronica determinato.

- **Intervallo di date:** questa opzione limita il rapporto a un intervallo di date determinato.

Una volta selezionate le opzioni del rapporto, fare clic sul pulsante **Rapporto** per generare il rapporto.

Statistiche di utilizzo del dominio

Il rapporto sulle statistiche di utilizzo del dominio offre una panoramica sulla quantità e sulla dimensione dei messaggi di posta elettronica inviati o ricevuti per domini non locali.



Schermata 18 - Finestra di dialogo del filtro per le statistiche di utilizzo del dominio

Tipo di rapporto

- **Tipo di rapporto: Per impostazione predefinita**, i dati del rapporto sulle statistiche di utilizzo del dominio sono validi sempre per i messaggi di posta elettronica in arrivo e in uscita.

Opzioni del rapporto

- **Ordina per:** consente di specificare se il rapporto deve essere ordinato per nome del dominio, numero di messaggi di posta elettronica o dimensione totale dei messaggi di posta elettronica.
- **Domini selezionati:** permette di mettere in evidenza i domini che inviano o ricevono più di un determinato numero di messaggi di posta elettronica o di una determinata quantità di megabyte di messaggi di posta elettronica.
- **Inizio elenco:** permette di elencare soltanto i primi domini del

rapporto.

- **Rapporto multi pagine:** permette di specificare il numero di domini che si desidera visualizzare su ogni pagina.

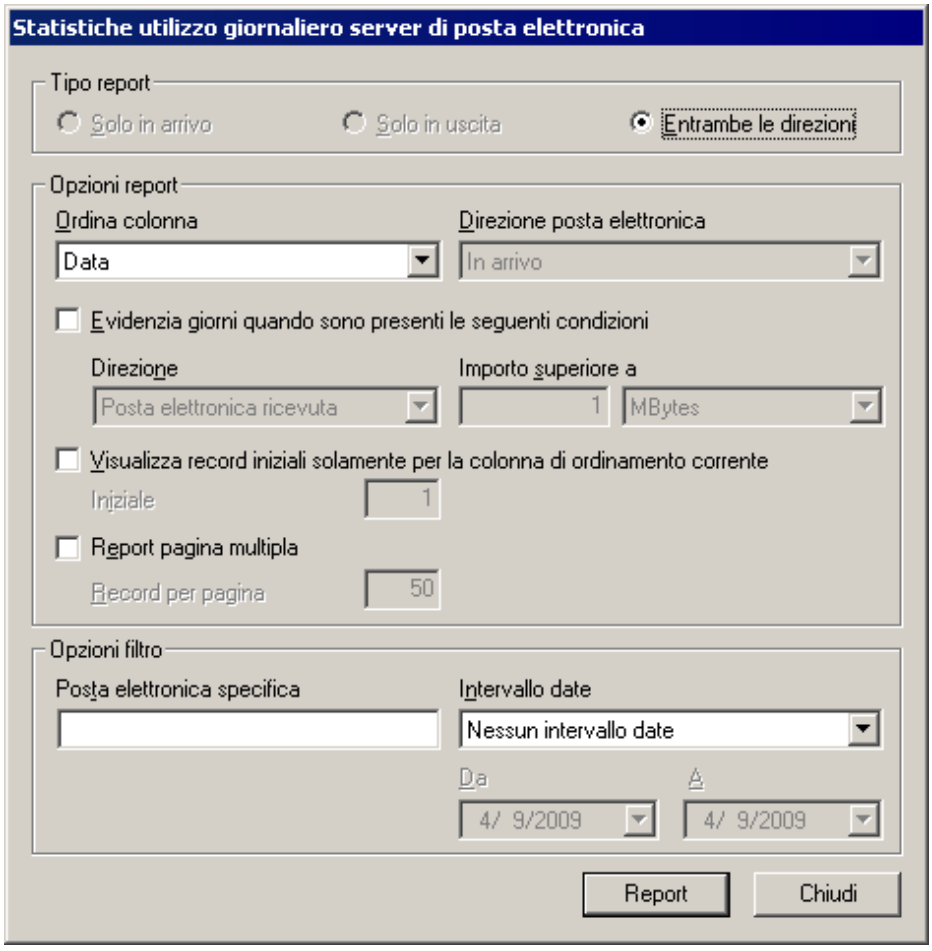
Opzioni di filtro

- **Dominio specifico:** questa opzione limita il rapporto a un dominio determinato.
- **Intervallo di date:** questa opzione limita il rapporto a un intervallo di date determinato.

Una volta selezionate le opzioni del rapporto, fare clic sul pulsante **Rapporto** per generare il rapporto.

Statistiche di utilizzo giornaliero del server di posta

Il rapporto sulle statistiche di utilizzo giornaliero del server di posta offre una panoramica sulla quantità di messaggi di posta elettronica inviati o ricevuti, al giorno, dal server di posta su cui è installato GFI MailEssentials.



Schermata 19 - Finestra di dialogo del filtro per le statistiche di utilizzo giornaliero del server di posta

Tipo di rapporto

- **Tipo di rapporto:** I dati sulle statistiche di utilizzo giornaliero del server di posta sono sempre riportati per i messaggi di posta elettronica in arrivo e in uscita.

Opzioni del rapporto

- **Ordina per:** permette di specificare se il rapporto deve essere ordinato per data (poiché il rapporto è giornaliero), per numero di messaggi di posta elettronica o dimensione totale dei messaggi di posta elettronica.
- **Giorni selezionati:** consente di mettere in evidenza i giorni nei quali si invia o riceve più di un determinato numero di messaggi di posta elettronica o di una determinata quantità di megabyte di messaggi di posta elettronica.
- **Inizio elenco:** permette di elencare soltanto i primi giorni del rapporto.
- **Rapporto multi pagine:** permette di specificare il numero di giorni che si desidera visualizzare su ogni pagina.

Opzioni di filtro

- **Indirizzo di posta elettronica specifico:** questa opzione limita il rapporto a un dominio determinato.
- **Intervallo di date:** questa opzione limita il rapporto a un intervallo di date determinato.

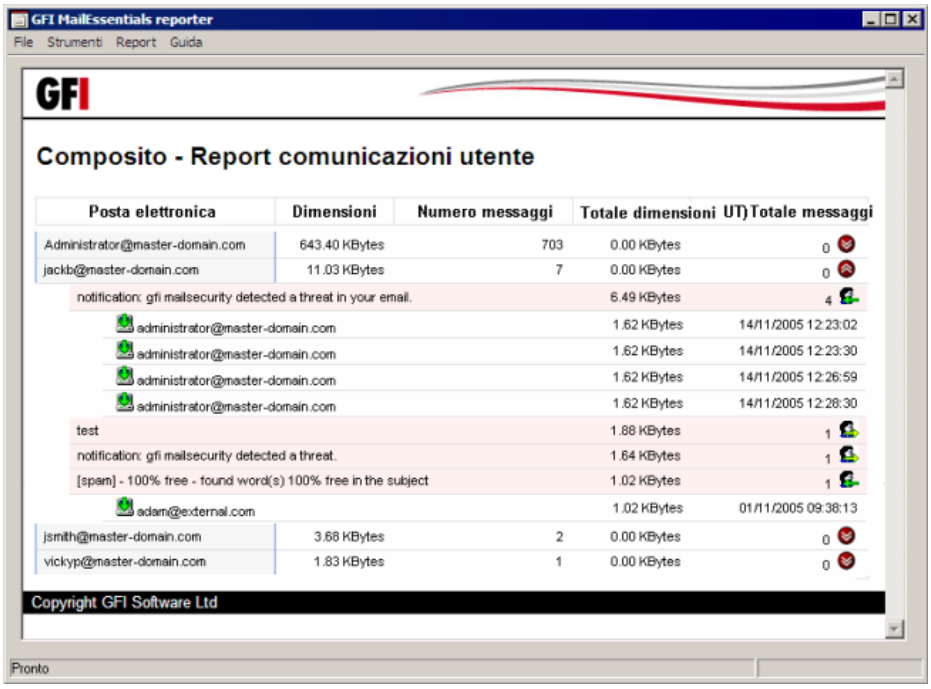
Una volta selezionate le opzioni del rapporto, fare clic sul pulsante **Rapporto** per generare il rapporto.

Comunicazioni dell'utente

Il rapporto sulle comunicazioni dell'utente permette di rivedere quali tipi di messaggi di posta elettronica sono stati inviati da ciascun utente. Una volta che si genera un rapporto sulle comunicazioni dell'utente, è possibile espandere il registro dell'utente per elencare l'oggetto dei messaggi di posta elettronica inviati o ricevuti. La posta avente lo stesso oggetto viene raggruppata. Questi messaggi di posta elettronica possono essere ulteriormente espansi per rivelare quando e a chi è stata inviata la posta con quell'oggetto.

Note importanti

1. Si tratta di un rapporto complesso che potrebbe richiedere tempo per la sua creazione. Si consiglia di limitare l'intervallo a un utente specifico o a un intervallo di date particolare.



Schermata 20 - Il rapporto sulle comunicazioni dell'utente visualizza l'esatto percorso del messaggio di posta elettronica.

Tipo di rapporto

- **Tipo di rapporto:** permette di indicare se si desidera generare un rapporto sui messaggi di posta elettronica in arrivo, in uscita o su entrambi.

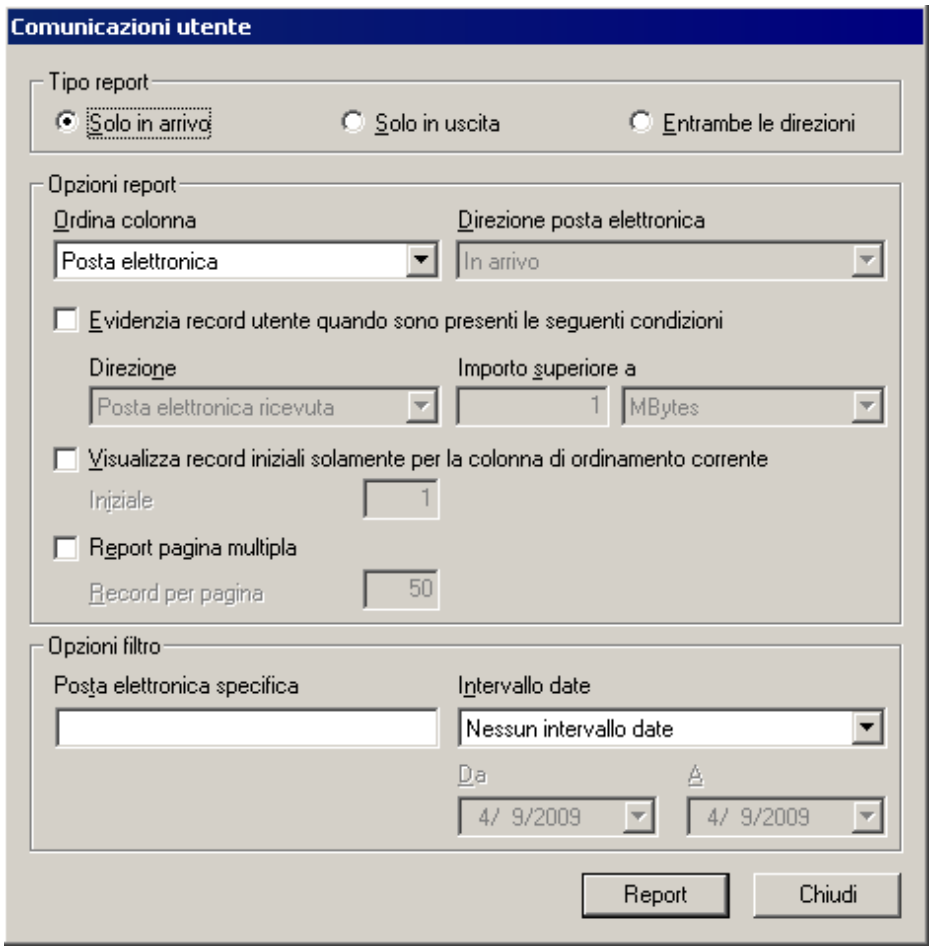
Opzioni del rapporto

- **Ordina per:** consente di specificare se il rapporto deve essere ordinato per indirizzo di posta elettronica, numero di messaggi di posta elettronica o dimensione totale dei messaggi di posta elettronica.
- **Utenti selezionati:** permette di mettere in evidenza gli utenti che hanno inviato o ricevuto più di un determinato numero di messaggi di posta elettronica o di una determinata quantità di megabyte di messaggi di posta elettronica.
- **Inizio elenco:** permette di elencare soltanto il numero specifico dei primi utenti del rapporto.
- **Rapporto multi pagine:** permette di specificare il numero di utenti che si desidera visualizzare su ogni pagina.

Opzioni di filtro

- **Indirizzo di posta elettronica specifico:** questa opzione limita il rapporto a un indirizzo di posta elettronica determinato.
- **Intervallo di date:** questa opzione limita il rapporto a un intervallo di date determinato.

Una volta selezionate le opzioni richieste, fare clic sul pulsante **Rapporto** per generare il rapporto.



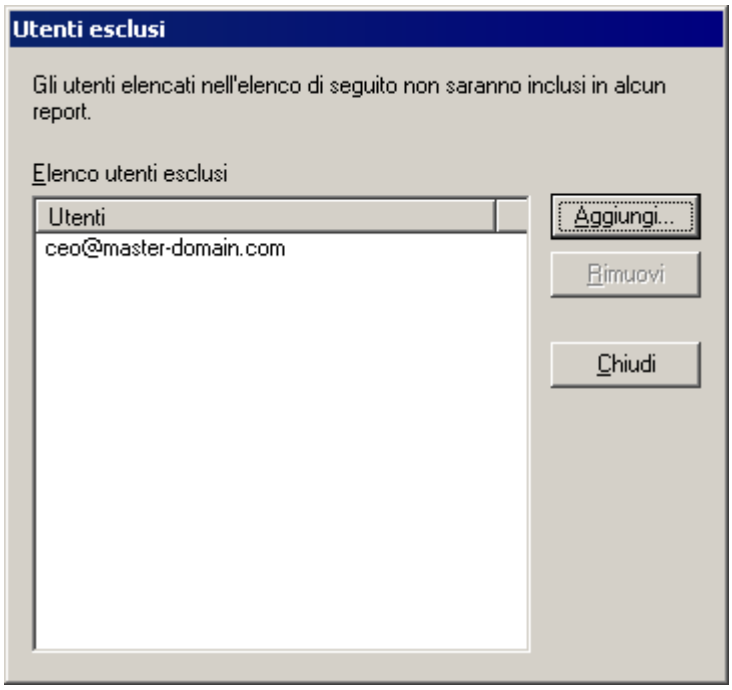
Schermata 21 - Finestra di dialogo del filtro per le comunicazioni dell'utente

Opzioni varie

- **Utenti esclusi dai rapporti**

  Lo strumento degli utenti esclusi permette di specificare gli indirizzi di posta elettronica che devono essere esclusi dai rapporti.

  Per escludere un utente andare su **Strumenti ► Elenco utenti esclusi**, fare clic sul pulsante **Aggiungi…** e **Aggiungi** o **Rimuovi** l'indirizzo di posta elettronica SMTP dell'utente da escludere dai rapporti.

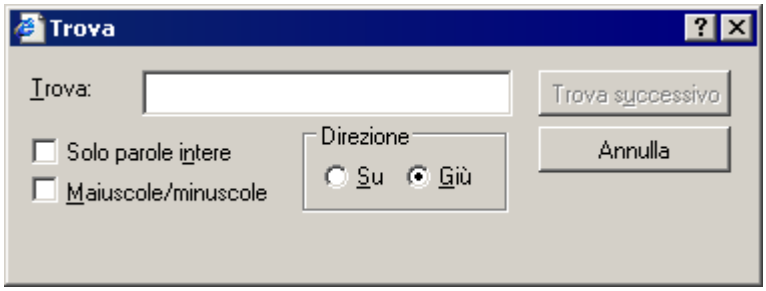


Schermata 22 - Finestra di dialogo degli utenti esclusi

- **Strumento "Trova"**

  Lo strumento "Trova" consente di cercare una stringa in un rapporto.

  Dall'opzione **Strumenti ► Trova**, inserire le stringhe da trovare e selezionare **Trova successivo** per cercare le stringhe.



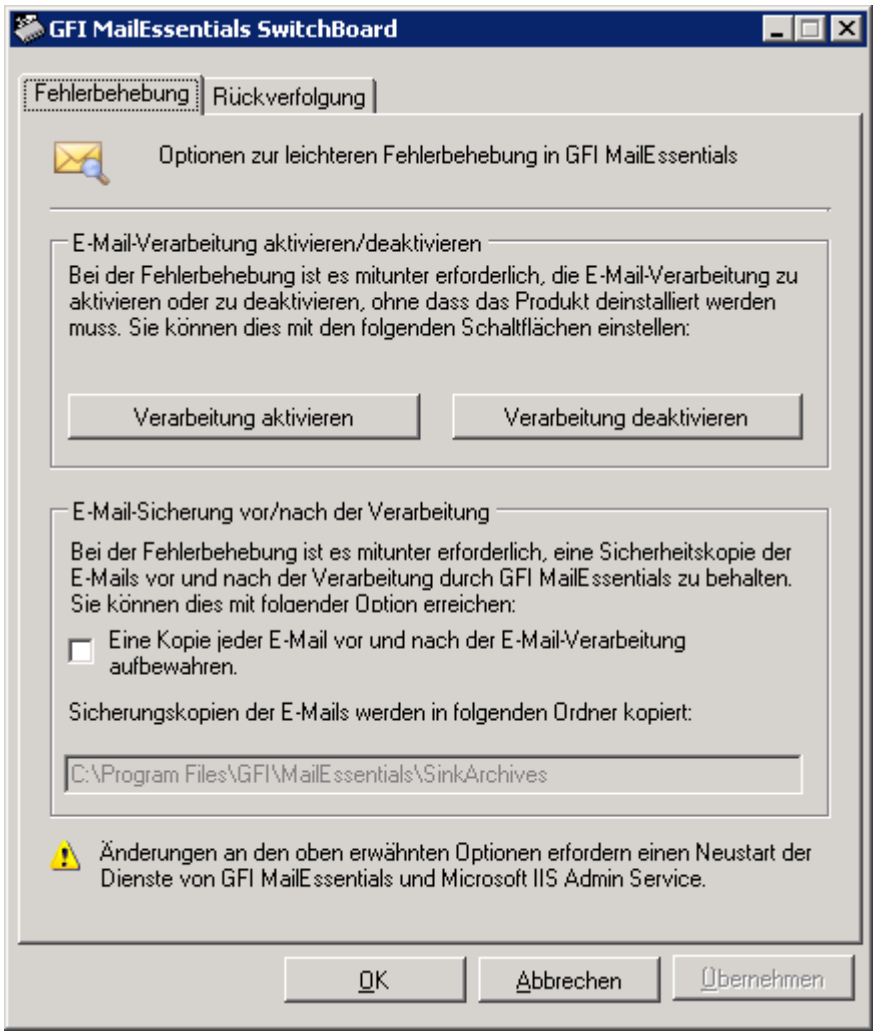
Schermata 23 - Finestra di dialogo Trova

3.8 Abilitazione/Disabilitazione dell' elaborazione dei messaggi di posta elettronica

Disabilitando la elaborazione dei messaggi di posta elettronica viene disabilitata tutta la protezione offerta da GFI MailEssentials e tutti i messaggi di posta elettronica (compreso lo spam) arrivano nelle cassette postali degli utenti.

Per abilitare/disabilitare l' elaborazione dei messaggi di posta elettronica da parte di GFI MailEssentials:

1. Andare su **Start ► Programmi ► GFI MailEssentials ► GFI MailEssentials Switchboard**.



Schermata 5 - GFI MailEssentials Switchboard: Risoluzione dei problemi

2. Dalla scheda **Risoluzione dei problemi** fare clic su:

- **Disabilita elaborazione** per disabilitare la scansione dei messaggi di posta elettronica
- **Abilita elaborazione** per abilitare la scansione dei messaggi di posta elettronica

L' elaborazione dei messaggi di posta elettronica può essere abilitata/disabilitata mediante finestra di comando. Per maggiori informazioni, consultare:

http://kbase.gfi.com/showarticle.asp?id=KBID003468.

4 Personalizzazione di GFI MailEssentials

4.1 Aggiunta di domini di posta elettronica in arrivo

I domini di posta elettronica in arrivo consentono a GFI MailEssentials di distinguere tra posta elettronica in arrivo e in uscita e di conseguenza individuare quali messaggi di posta elettronica devono essere sottoposti a scansione per individuare lo spam. Durante l'installazione, i domini di posta elettronica in arrivo sono importati dal servizio SMTP IIS .

In alcuni casi, tuttavia, l'indirizzamento della posta elettronica locale verso IIS potrebbe richiedere una configurazione diversa.

- **Esempio:** aggiungere domini che sono locali ai fini dell'indirizzamento della posta elettronica ma non sono locali per il server di posta in uso.

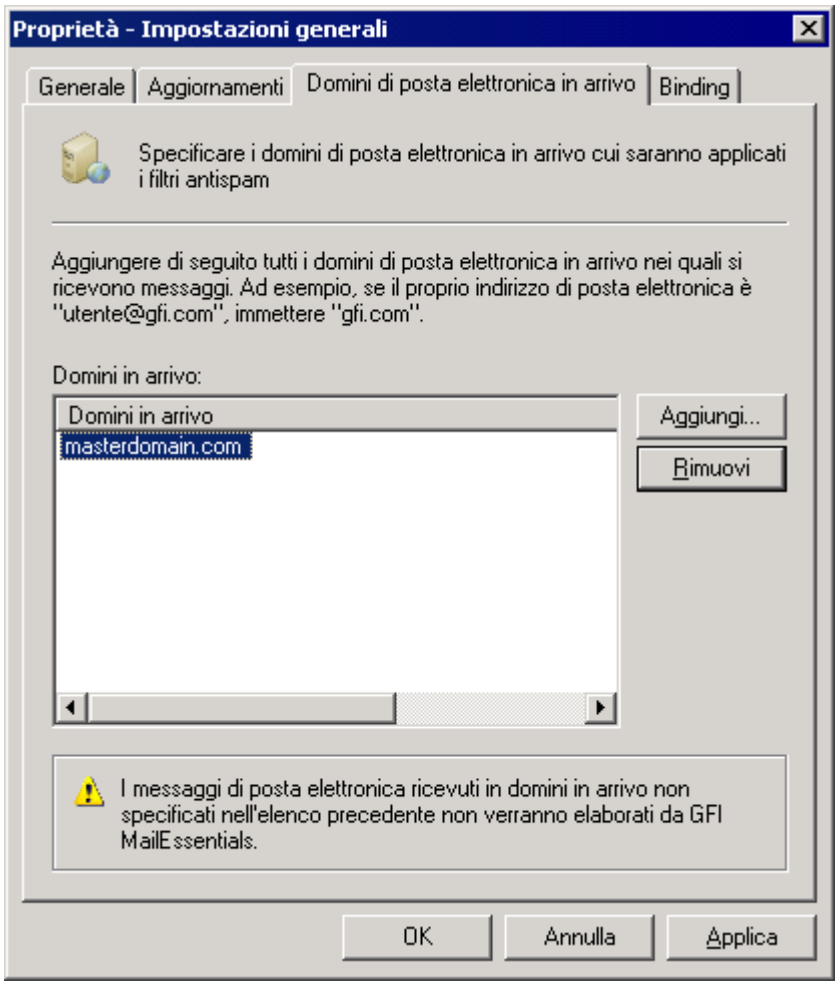
Le istruzioni nella presente sezione mostrano come aggiungere o rimuovere i domini di posta elettronica in arrivo dopo l'installazione.

Note importanti

1. Qualsiasi dominio su cui viene ricevuta la posta elettronica non elencato nella configurazione dei domini di posta elettronica in arrivo non è protetto da GFI MailEssentials contro lo spam.

4.1.1 Aggiunta e rimozione di domini in arrivo

1. Fare clic con il pulsante destro del mouse sul nodo **Generale ► Impostazioni generali**, selezionare **Proprietà** e fare clic sulla scheda **Domini di posta elettronica in arrivo**.



Schermata 24 - Aggiunta di un dominio di posta elettronica in arrivo

2. Fare clic sul pulsante **Aggiungi…** e inserire i dettagli del dominio per aggiungere un nuovo dominio di posta elettronica in arrivo. Per rimuovere i domini, selezionare il dominio da rimuovere e fare clic su **Rimuovere**.

3. Fare clic su **OK** per completare le impostazioni.

4.2 Filtri antispam

GFI MailEssentials adopera vari filtri di scansione per individuare lo spam:

Filtro	Descrizione	Attivato per impostazione predefinita
SpamRazer	Un motore antispam che stabilisce se un messaggio di posta elettronica è uno spam utilizzando la reputazione dei messaggi, le impronte digitali dei messaggi e l'analisi dei contenuti.	Si
Raccolta di directory	Blocca un messaggio di posta elettronica che viene casualmente generato verso un server e inviato prevalentemente a utenti non esistenti.	Si
Phishing	Blocca i messaggi di posta elettronica contenenti nel corpo del messaggio link a siti di phishing noti o parole chiave tipiche	Si

	dell'attività di phishing.	
Sender Policy Framework	Ferma messaggi di posta elettronica provenienti da domini non autorizzati secondo i registri Sender Policy Framework.	No
White list automatica	Gli indirizzi a cui un messaggio di posta elettronica viene inviato sono automaticamente esclusi dal blocco.	Si
White list	Un elenco personalizzato di indirizzi di posta elettronica sicuri.	Si
Black list dei messaggi di posta elettronica	Un elenco personalizzato di utenti o domini di posta elettronica bloccati.	Si
Black list DNS	Verifica se il messaggio di posta elettronica proviene dai mittenti presenti in una black list DNS pubblica di spammer noti.	Si
Block list di URI anti-spam in tempo reale	Ferma messaggi di posta elettronica che contengono link a domini presenti su Blocklist antispam di URI pubbliche come sc.surbl.org.	Si
Controllo intestazioni	Un modulo che analizza i singoli campi di un'intestazione relazionandoli ai campi SMTP e MIME.	Si
Controllo parola chiave	I messaggi di spam sono individuati sulla base di parole chiave bloccate nel titolo o nel corpo del messaggio di posta elettronica.	No
Nuovi mittenti	Messaggi di posta elettronica ricevuti da mittenti a cui non erano mai stati inviati messaggi prima d'ora.	No
Analisi bayesiana	Una tecnica antispam dove un indice di probabilità statistica basata sulla formazione degli utenti viene usata per individuare lo spam.	No

4.2.1 Azioni antispam

GFI MailEssentials può intraprendere alcune azioni quando un messaggio viene identificato come spam. Queste azioni comprendono:

- eliminazione del messaggio;
- spostamento del messaggio verso una cartella centrale;
- inoltro verso un indirizzo di posta elettronica;
- etichettatura della posta;
- spostamento del messaggio verso la cartella Posta indesiderata.

NOTA: per informazioni dettagliate sulle azioni antispam, consultare la sezione Azioni antispam: cosa fare dei messaggi di spam a pagina 73 del presente manuale.

4.2.2 SpamRazer

SpamRazer è il motore antispam primario di GFI abilitato per impostazione predefinita all'installazione. Vengono realizzati frequenti

aggiornamenti per SpamRazer per migliorare i tempi di risposta alle nuove evoluzioni dello spam.

NOTA: SpamRazer è anche il motore antispam che blocca lo spam NDR. Per maggiori informazioni su GFI MailEssentials e lo spam NDR, consultare:

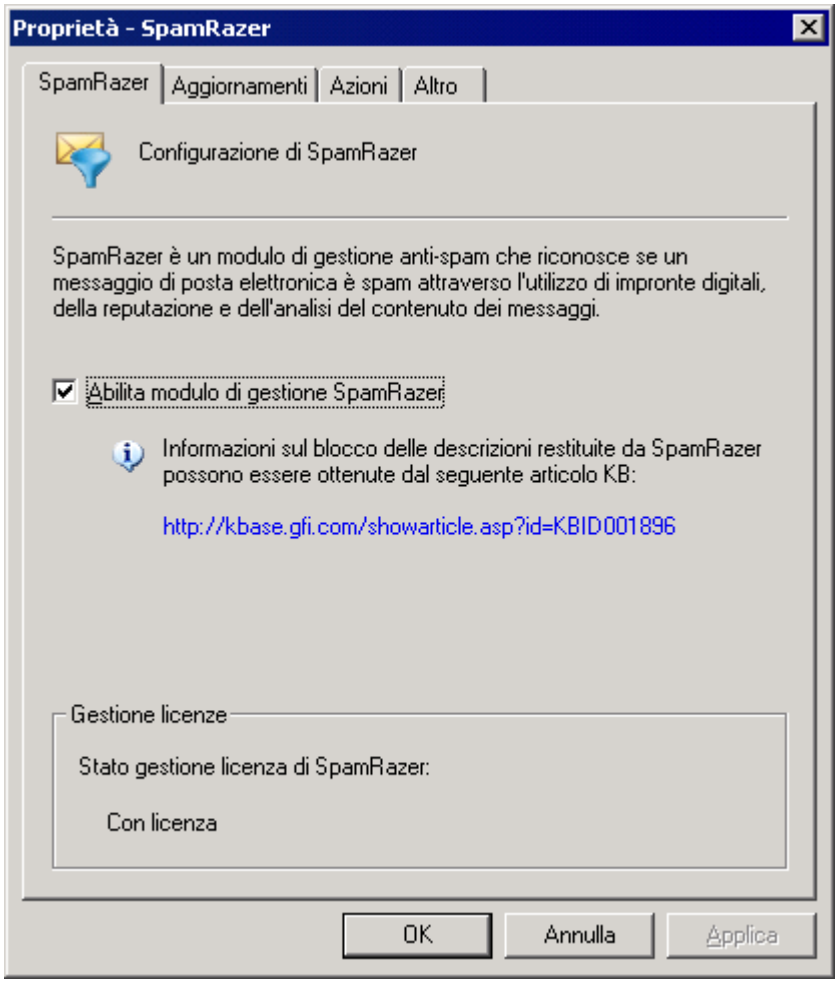
http://kbase.gfi.com/showarticle.asp?id=KBID003322

Configurazione di SpamRazer

NOTA 1: la disabilitazione di SpamRazer NON è raccomandata.

NOTA 2: GFI MailEssentials scarica gli aggiornamenti per SpamRazer da: http://sn92.mailshell.net

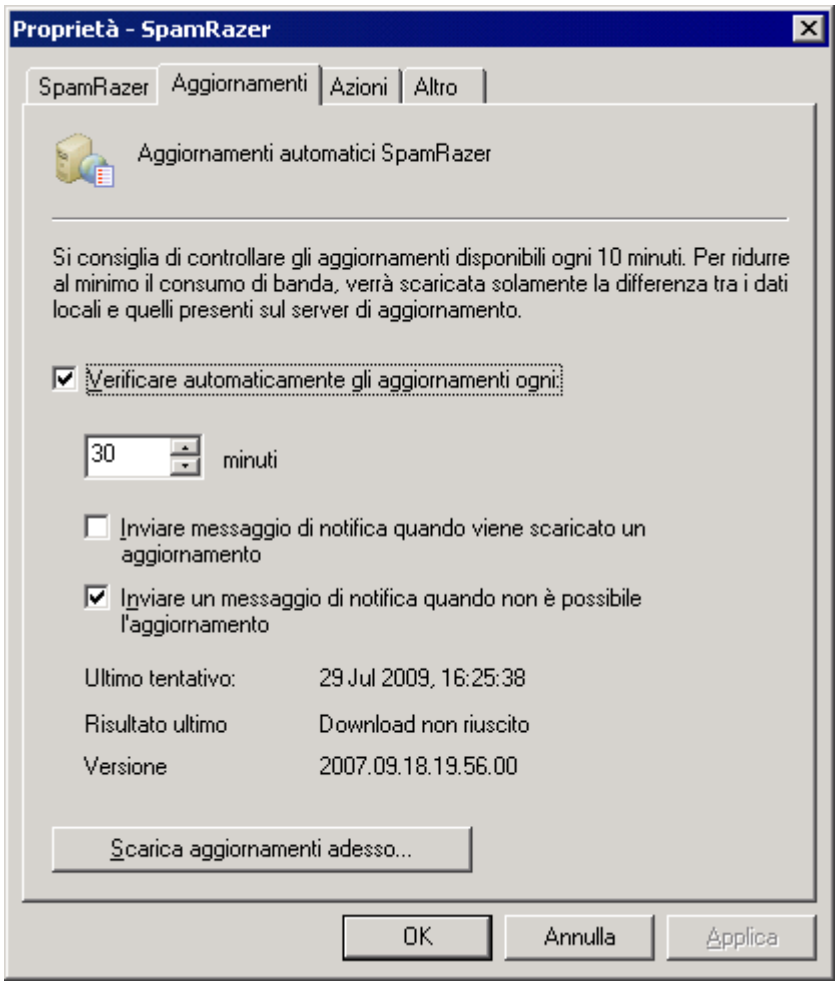
1. Selezionare **AntiSpam ► Filtri Antispam ► SpamRazer ► Proprietà.**



Schermata 25 - Proprietà SpamRazer

2. Dalla scheda **SpamRazer** eseguire una delle seguenti azioni:

- Selezionare/deselezionare la casella di controllo **Abilita motore SpamRazer** per abilitare o disabilitare SpamRazer.



Schermata 26 - Aggiornamenti automatici per SpamRazer

3. Dalla scheda **Aggiornamenti** eseguire una delle seguenti azioni:

- Selezionare/deselezionare la casella di controllo **Verifica automatica degli aggiornamenti** per configurare GFI MailEssentials per la verifica e lo scaricamento automatico degli aggiornamenti .per SpamRazer. Specificare l'intervallo di tempo in minuti per la verifica degli aggiornamenti.

  NOTA: si raccomanda di lasciare attivata questa opzione affinché SpamRazer sia più efficace nel rilevamento dei nuovi spam.

- Selezionare/deselezionare la casella di controllo **Invia un messaggio di notifica al termine di un aggiornamento** per ricevere informazioni mediante posta elettronica quando sono stati scaricati nuovi aggiornamenti .

- Selezionare/deselezionare la casella di controllo **Invia un messaggio di notifica quando un aggiornamento non è riuscito** per ricevere informazioni quando uno scaricamento o un'installazione non vengono portati a termine.

- Fare clic su **Scarica aggiornamenti adesso**… per scaricare gli aggiornamenti.

NOTA: Per scaricare gli aggiornamenti con un server proxy consultare Configurazione aggiornamenti automatici a pagina 116 di questo manuale.

4. Fare clic sulla scheda **Azioni** o **Altro** per selezionare le azioni da

eseguire sui messaggi individuati come spam. Per maggiori informazioni, consultare la sezione Azioni antispam: cosa fare dei messaggi di spam a pagina 73 del presente manuale. Fare clic su **OK** per completare la configurazione.

4.2.3 Phishing

Il phishing è una tecnica utilizzata dai cosiddetti spammer per eseguire azioni fraudolente mediante la posta elettronica allo scopo di ottenere dagli utenti della posta elettronica dati personali. Un messaggio di posta elettronica di phishing sarà creato in modo da apparire come un messaggio formale proveniente da un'azienda seria, per esempio, una banca. I messaggi di posta elettronica di phishing contengono di solito istruzioni, per esempio, con cui la banca richiede di riconfermare nome utente e password utilizzate per il collegamento con l'home banking oppure informazioni sulla carta di credito. I messaggi di posta elettronica di phishing contengono solitamente un URI (Uniform Resource Identifier) di phishing che l'utente dovrebbe seguire per inserire alcuni dati sensibili su un sito. Il sito a cui si viene indirizzati dall'URI di phishing appare come il sito ufficiale, ma in realtà è controllato da colui che ha inviato il messaggio di posta elettronica di phishing. Quando l'utente inserisce i dati sensibili sul sito di phishing, questi dati sono raccolti e quindi utilizzati, per esempio, per prelevare denaro dal conto corrente bancario dell'utente preso di mira.

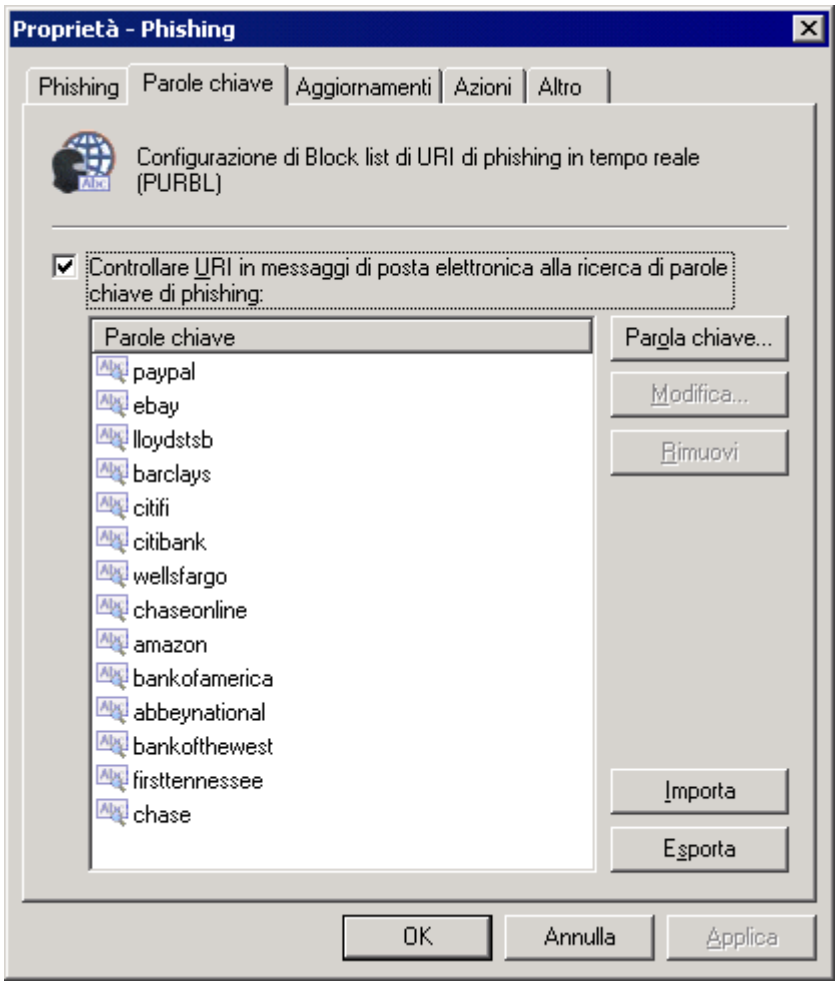
La caratteristica delle Phishing individua i messaggi di posta elettronica di phishing confrontando gli URI presenti nella posta elettronica con un data base di URI noti per essere stati utilizzati in attacchi di phishing e, inoltre, cercando negli URI parole chiave tipiche del phishing.

Il filtro Phishing è attivato per impostazione predefinita all'installazione.

Configurazione della Phishing

NOTA 1: la disabilitazione della Phishing NON è raccomandata.

1. Selezionare **AntiSpam ► Filtri Antispam ► Phishing ► Proprietà.**



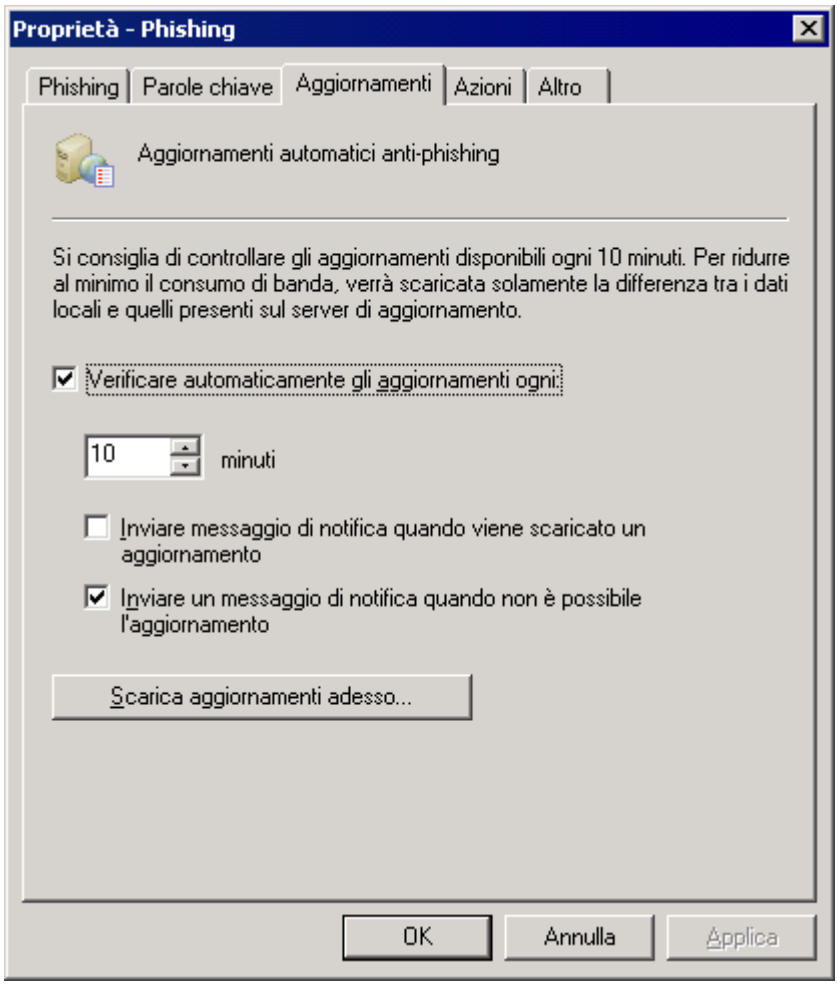
Schermata 27 - Parole chiave del phishing

2. Dalla scheda **Phishing** eseguire le azioni seguenti:

- Selezionare/deselezionare l'opzione **Verifica i messaggi di posta ai fini della presenza di URI a siti di phishing conosciuti** per abilitare/disabilitare la Phishing.

3. Dalla scheda **Parole chiave** eseguire le seguenti azioni:

- Selezionare/deselezionare l'opzione **Ricerca parole chiave tipiche del phishing degli URI presenti nei messaggi di posta** per abilitare/disabilitare le parole chiave tipiche del phishing.
- Fare clic sul pulsante **Parola chiave** e inserire le parole chiave nella finestra di dialogo **Inserisci una parola chiave** per aggiungere parole chiave al filtro Phishing.
- Selezionare una parola chiave e fare clic su **Modifica** o **Rimuovi** per modificare o rimuovere una parola chiave precedentemente inserita nel filtro Phishing.
- Fare clic su **Esporta** per esportare la lista attuale delle parole chiave in formato XML.
- Fare clic sul pulsante **Importa** per importare una lista di parole chiave precedentemente esportata in XML.



Schermata 28 - Aggiornamenti automatici antiphishing

4. Dalla scheda **Aggiornamenti** eseguire una delle seguenti azioni:

- Selezionare/deselezionare la casella di controllo **Verifica automatica degli aggiornamenti** per abilitare o disabilitare la verifica e lo scaricamento automatici degli aggiornamenti antiphishing.

  NOTA: si raccomanda di lasciare attivata questa opzione affinché aggiornamenti frequenti consentano alla Phishing di essere più efficace nel rilevamento di nuovi messaggi di posta elettronica di phishing.

- Selezionare/deselezionare la casella di controllo **Invia un messaggio di notifica al termine di un aggiornamento** per ricevere informazioni mediante posta elettronica quando sono stati scaricati nuovi aggiornamenti.

- Selezionare/deselezionare la casella di controllo **Invia un messaggio di notifica quando un aggiornamento non è riuscito** per ricevere informazioni quando uno scaricamento o un'installazione non vengono portati a termine.

NOTA: Per scaricare gli aggiornamenti con un server proxy consultare Configurazione aggiornamenti automatici a pagina 116 di questo manuale.

5. Fare clic sulla scheda **Azioni** o **Altro** per selezionare le azioni da eseguire sui messaggi individuati come phishing. Per maggiori

informazioni, consultare la sezione Azioni antispam: cosa fare dei messaggi di spam a pagina 73 del presente manuale. Fare clic su **OK** per completare la configurazione.

4.2.4 Filtro Sender Policy Framework (SPF)

Il filtro Sender Policy Framework è uno sforzo comune che richiede che i mittenti abbiano pubblicato il proprio server di posta in un registro SPF. Il filtro rileva mittenti manomessi.

- **Esempio:** se un messaggio di posta elettronica è inviato da xyz@CompanyABC.com, la società "companyABC.com" deve pubblicare un registro Sender Policy Framework affinché il protocollo Sender Policy Framework possa determinare se il messaggio di posta elettronica sia stato davvero inviato dalla rete di "companyABC.com" o se sia stato falsificato. Se l'azienda CompanyABC.com non pubblica alcun registro Sender Policy Framework, il risultato del protocollo Sender Policy Framework sarà "sconosciuto".

Per maggiori informazioni su Sender Policy Framework e sul suo funzionamento, è possibile consultare il sito Web di Sender Policy Framework: http://www.openspf.org.

Il filtro Sender Policy Framework NON è abilitato per impostazione predefinita e andrebbe abilitato esclusivamente nei casi in cui si reputa elevata la minaccia di mittenti manomessi.

GFI MailEssentials non rende obbligatoria la pubblicazione dei registri Sender Policy Framework. Per la pubblicazione dei registri Sender Policy Framework, utilizzare la procedura guidata su:

http://www.openspf.org/wizard.html.

Prerequisiti

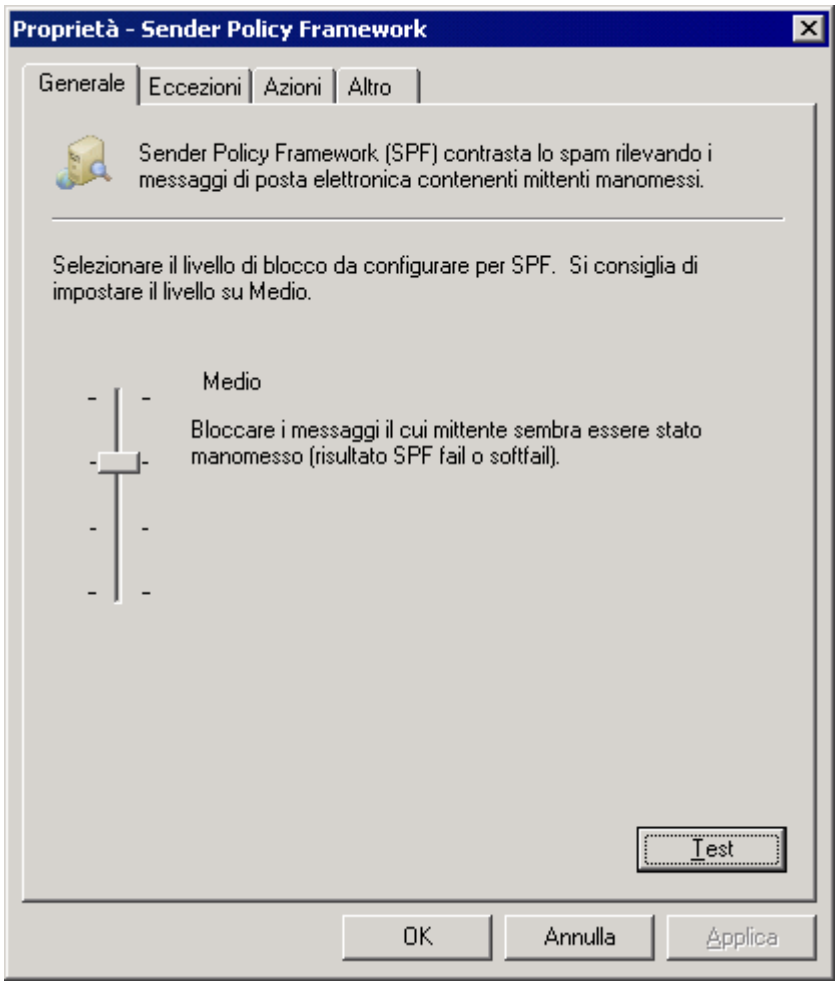
Prima di abilitare il filtro Sender Policy Framework su un'installazione server non-gateway:

1. Fare clic con il tasto destro del mouse su **Antispam ► Impostazioni Antispam ► Proprietà** e selezionare la scheda **Server STMP perimetrali**.

2. Fare clic sul pulsante **Riconoscimento automatico** presente nell'opzione della configurazione "SMTP perimetrale", per eseguire una ricerca MX DSN e definire automaticamente l'indirizzo IP del server SMTP perimetrale.

Configurazione del filtro Sender Policy Framework

1. Selezionare **Antispam ► Filtri Antispam ► Sender Policy Framework ► Proprietà.**



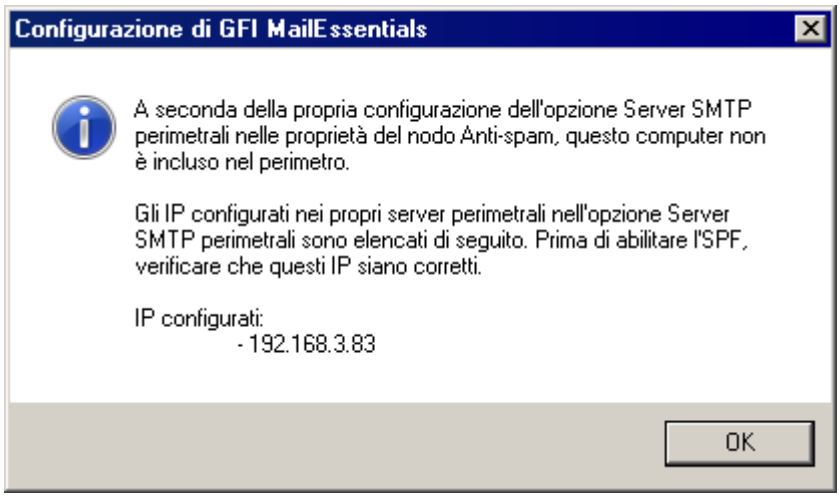
Schermata 29 - Configurazione del livello di blocco Sender Policy Framework

2. Definire la sensibilità del controllo Sender Policy Framework usando lo slider e fare clic su **Applica**. Si può scegliere fra quattro livelli:

- **Mai**: Non bloccare mai i messaggi. I controlli Sender Policy Framework non vengono effettuati.
- **Basso:** Bloccare solo i messaggi il cui mittente risulta essere manomesso. Questa opzione tratta come spam i messaggi con mittenti manomessi.
- **Medio:** Bloccare i messaggi il cui mittente sembra essere stato manomesso. Questa opzione tratta come spam tutti i messaggi che sembrano provenire da mittenti manomessi.

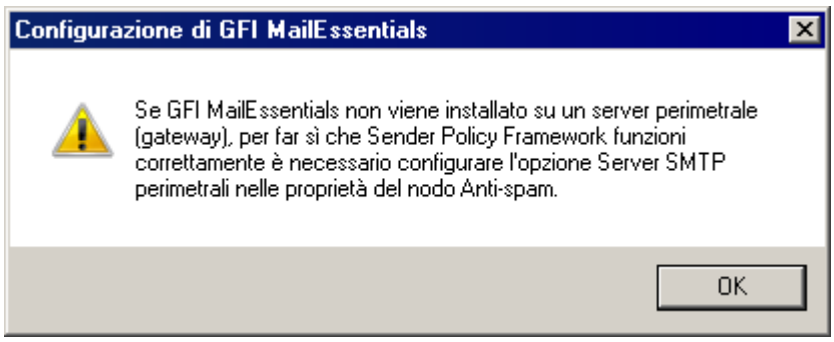
  NOTA: si tratta dell'impostazione predefinita consigliata.
- **Alto:** Blocca i messaggi il cui invio da parte del mittente non è stato provato. Questa opzione tratta tutti i messaggi di posta elettronica come spam, a meno che non sia possibile provare che il mittente non è stato manomesso.

  NOTA: poiché la maggioranza dei server di posta non hanno ancora un registro Sender Policy Framework, tale opzione non è per ora consigliata.



Schermata 30 - Configurazione dell'attuale server SMTP perimetrale

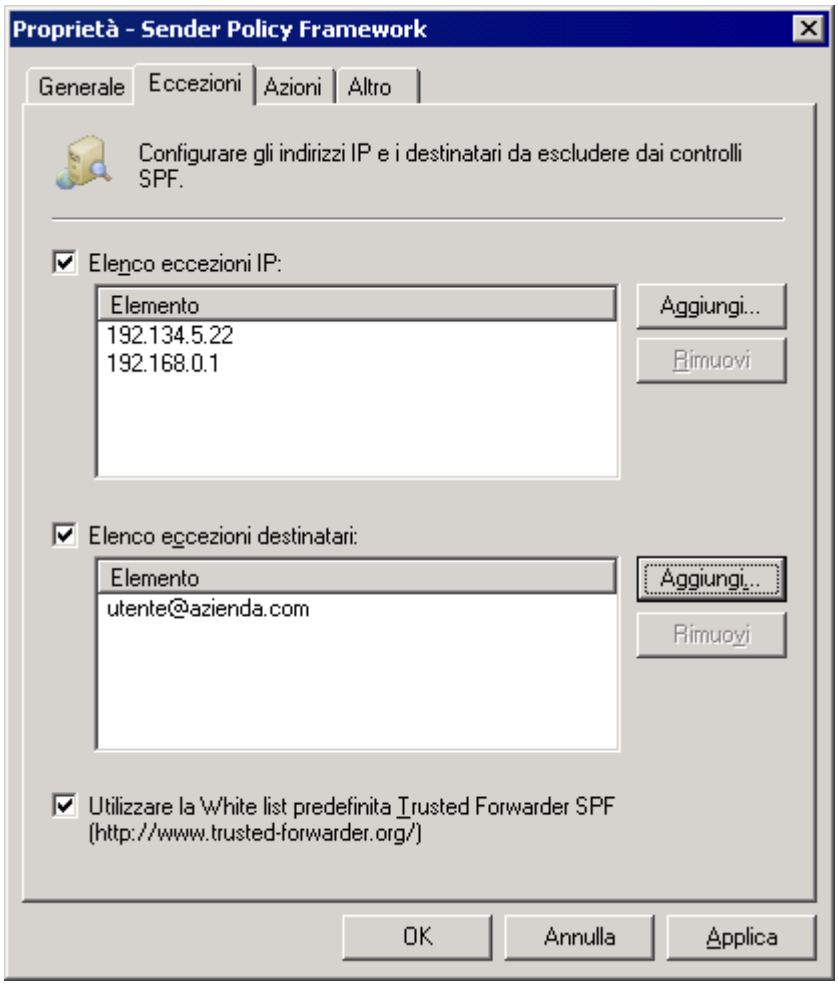
3. Se questo computer **NON** costituisce il server SMTP perimetrale, compare una finestra di dialogo che mostra le impostazioni del server SMTP perimetrale precedentemente configurate (cioè, gli indirizzi IP specificati per il proprio server SMTP perimetrale).



Schermata 31 - Promemoria: Sender Policy Framework deve essere installato sul server SMTP perimetrale.

4. Se GFI MailEssentials è installato sul server SMTP perimetrale o se non si è ancora specificato che il server di posta che esegue GFI MailEssentials NON è un server SMTP perimetrale, comparirà una finestra di dialogo. Configurare l'opzione **Server SMTP perimetrali** nelle proprietà del nodo Antispam (fare clic con il pulsante destro del mouse sulla scheda **AntiSpam ► Impostazioni antispam ► Proprietà ► Server SMTP perimetrali**).

5. Per provare i propri servizi o le proprie impostazioni DNS, fare clic sul pulsante **Prova**.



Schermata 32 - Configurazione delle eccezioni Sender Policy Framework

6. Selezionare la scheda **Eccezioni** per configurare gli indirizzi IP e i destinatari per escludere le verifiche Sender Policy Framework :

- **Elenco eccezioni di IP:** gli indirizzi IP di quest'elenco supereranno automaticamente i controlli Sender Policy Framework. Selezionare **Aggiungi** per aggiungere un nuovo indirizzo IP o selezionare gli indirizzi IP dall'elenco e fare clic sul pulsante **Rimuovi** per rimuoverli. Per disabilitare l'elenco delle eccezioni di IP, deselezionare la casella di controllo **Elenco eccezioni di IP**.
- **Elenco eccezioni di destinatari:** Questa opzione permette ad alcuni destinatari di ricevere sempre i messaggi di posta elettronica, anche se i messaggi andrebbero rifiutati. Per inserire un'eccezione di destinatario esistono tre modi:
  - parte locale - 'abuse' (corrisponde a 'abuse@abc.com', 'abuse@xyz.com', ecc...)
  - dominio - '@abc.com' (corrisponde a 'john@abc.com', 'jill@abc.com', ecc...)
  - completa - 'joe@abc.com' (corrisponde unicamente a 'joe@abc.com')

  Per disabilitare l'elenco delle eccezioni di destinatari, deselezionare la casella di controllo **Elenco eccezioni di destinatari**.

- **Trusted Forwarder Global Whitelist:** Questa white list (www.trusted-forwarder.org) fornisce agli utenti Sender Policy Framework una white list generale. Questa offre un modo per evitare che messaggi di posta elettronica legittimi inviati da mittenti di posta elettronica conosciuti e fidati vengano bloccati dai controlli SPF perché i mittenti non si avvalgono di sistemi di *envelope-from rewriting*.

  NOTA: tale impostazione è abilitata per impostazione predefinita. Si consiglia di lasciare sempre abilitata questa opzione.

7. Fare clic sulla scheda **Azioni** o **Altro** per selezionare le azioni da eseguire sui messaggi individuati come phishing. Per maggiori informazioni, consultare la sezione Azioni antispam: cosa fare dei messaggi di spam a pagina 73 del presente manuale. Fare clic su **OK** per completare la configurazione.

4.2.5 White list

La white list è un elenco di indirizzi di posta elettronica e domini dai quali si desidera sempre ricevere messaggi di posta elettronica. I messaggi di posta elettronica inviati da questi indirizzi o domini non saranno mai contrassegnati come spam. È inoltre possibile configurare parole chiave che, se presenti nel testo o nell'oggetto del messaggio di posta elettronica, determineranno l'inserimento automatico del messaggio di posta elettronica nella white list.

GFI MailEssentials presenta inoltre un'opzione di white list automatica che determina l'inserimento automatico degli indirizzi di posta elettronica nella white list ai quali si inviano i messaggi di posta elettronica. Ciò consente di ricevere i messaggi di posta elettronica dai destinatari dei messaggi di posta elettronica.

Le funzioni della white list e della white list automatica sono abilitate per impostazione predefinita all'installazione di GFI MailEssentials.

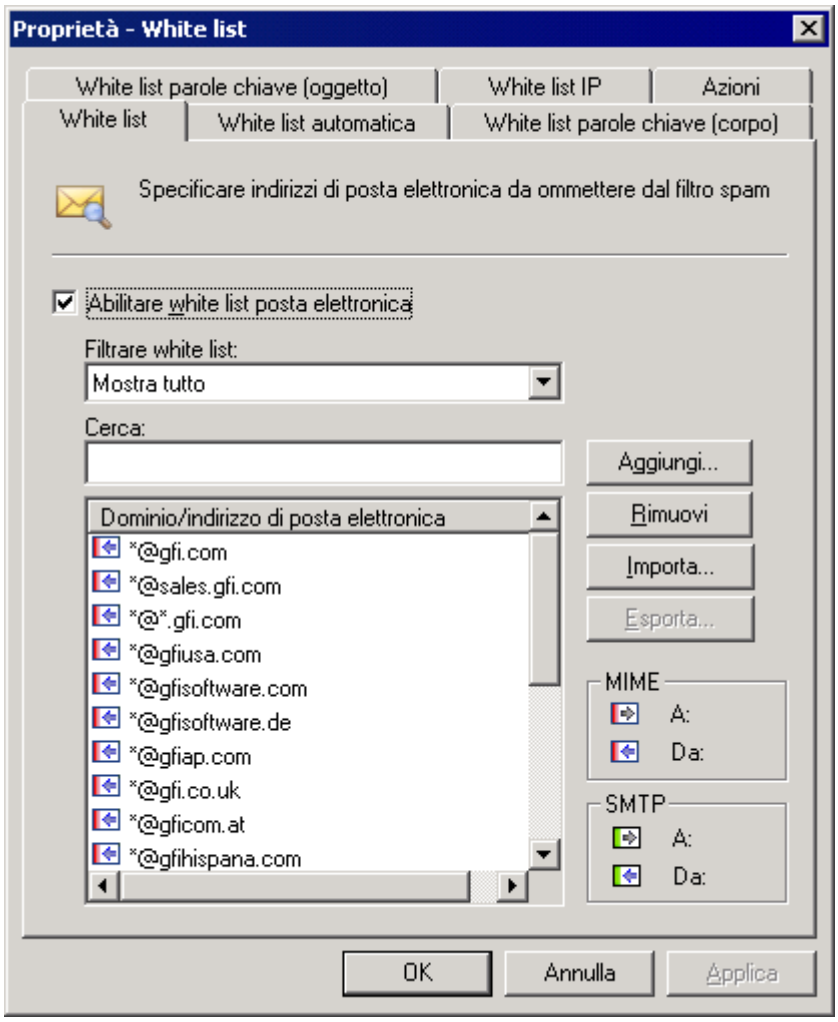
Note importanti

1. Si consiglia fortemente di lasciare abilitata questa caratteristica della white list poiché riduce la percentuale dei falsi positivi.

2. L'immissione di troppe parole chiave aumenta la possibilità che lo spam riesca a passare i filtri antispam.

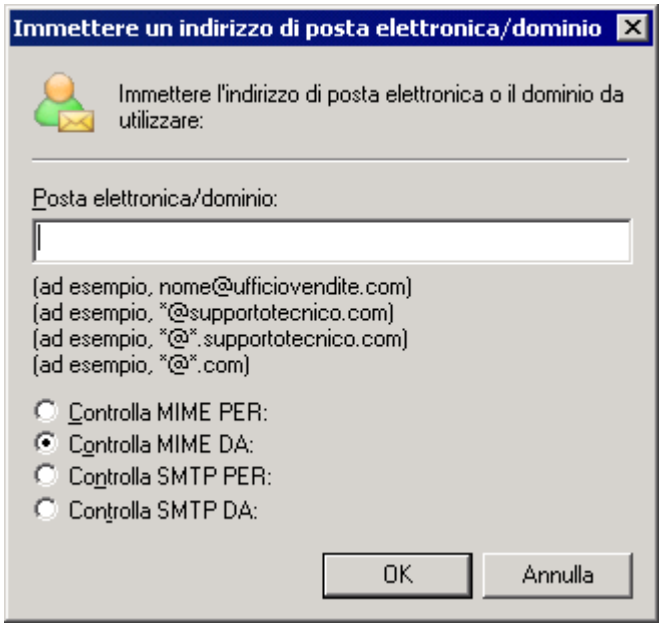
Configurazione della white list

1. Selezionare **Antispam ► White list ► Proprietà.**



Schermata 33 - Domini inseriti nella white list

2. Dalla scheda **White list**, aggiungere alla white list un dominio o un indirizzo di posta elettronica facendo clic su **Aggiungi**.



Schermata 34 - Aggiunta di un indirizzo di posta elettronica alla white list

3. Nella finestra di dialogo **Immettere un indirizzo di posta elettronica/dominio** specificare:

- indirizzo di posta elettronica completo; o
- indirizzi di posta elettronica di un intero dominio (per esempio: *@companysupport.com); o
- il suffisso di un intero dominio (per esempio: *@*.mil o *@*.edu)

  NOTA: quando vengono configurati i suffissi degli interi domini accertarsi che, per esempio, i messaggi di posta elettronica inviati da domini militari o didattici non saranno mai contrassegnati come spam.

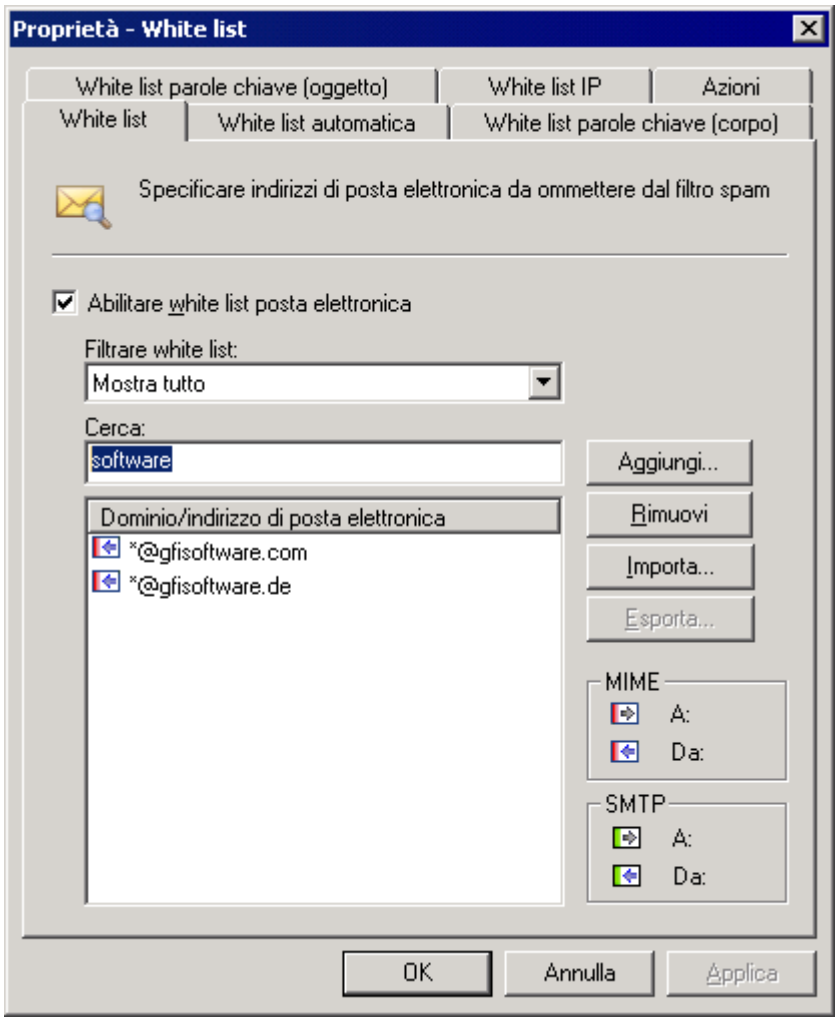
Per indicare inoltre a quale campo dell'intestazione del messaggio di posta elettronica deve corrispondere tale voce, in modo da poter inserire il messaggio in questione nella white list, fare clic su **Controlla…**.

- **Esempio:** per inserire nella white list tutti i messaggi di posta elettronica in arrivo inviati da un determinato utente, selezionare l'opzione **Controlla MIME DA** :

NOTA 1: alcune newsletter utilizzano *mailer* che non comprendono il mittente nel campo "MIME A:". Questo causa l'identificazione della posta elettronica come spam da parte della caratteristica di controllo delle intestazioni di GFI MailEssentials. Devono essere inserite nella white list con l'opzione **Controlla MIME A** :

NOTA 2: per escludere un utente locale dal filtraggio dello spam, è sufficiente inserire l'indirizzo di posta elettronica dell'utente e selezionare l'opzione **Controlla MIME A** :

Fare clic su **OK** per completare l'inserimento dell'indirizzo di posta elettronica/del dominio**.**



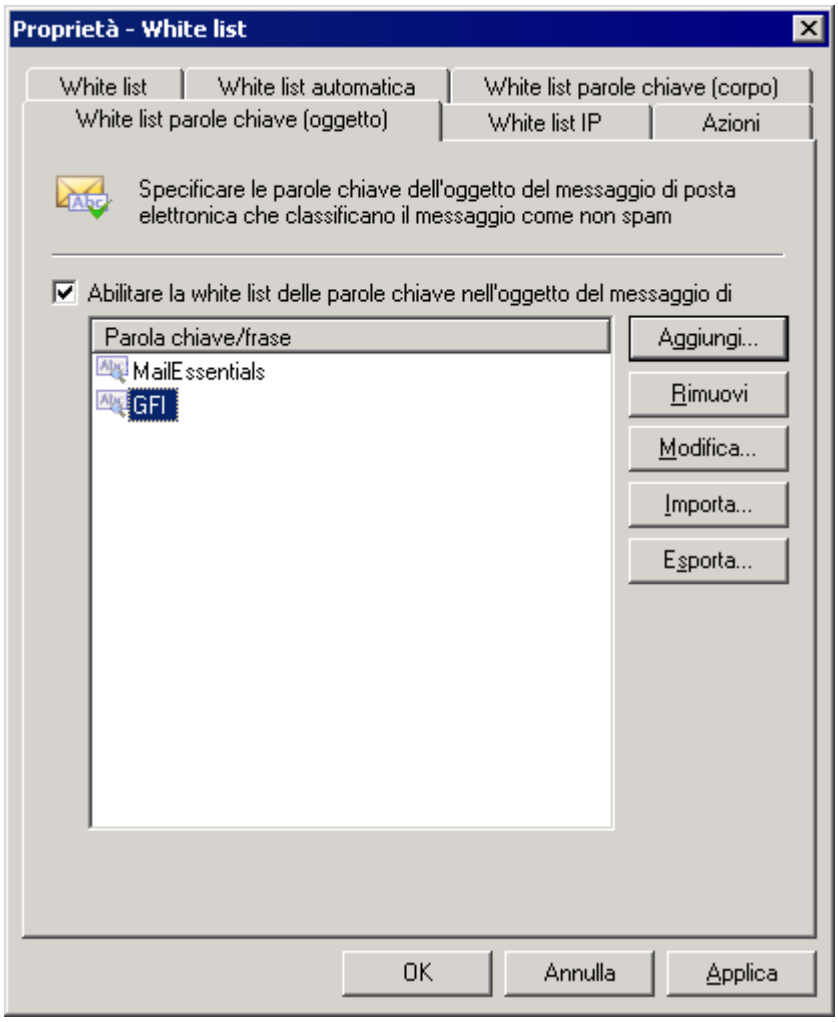
Schermata 6 - Ricerca indirizzi di posta elettronica e domini nella white list

4. Per ricercare indirizzi di posta elettronica e domini nella white list, digitare un criterio di ricerca nella casella di testo di **Ricerca**. Le voci corrispondenti saranno automaticamente visualizzate sotto.

5. Selezionare la scheda **White list automatica** per configurare le seguenti opzioni di white list automatica:

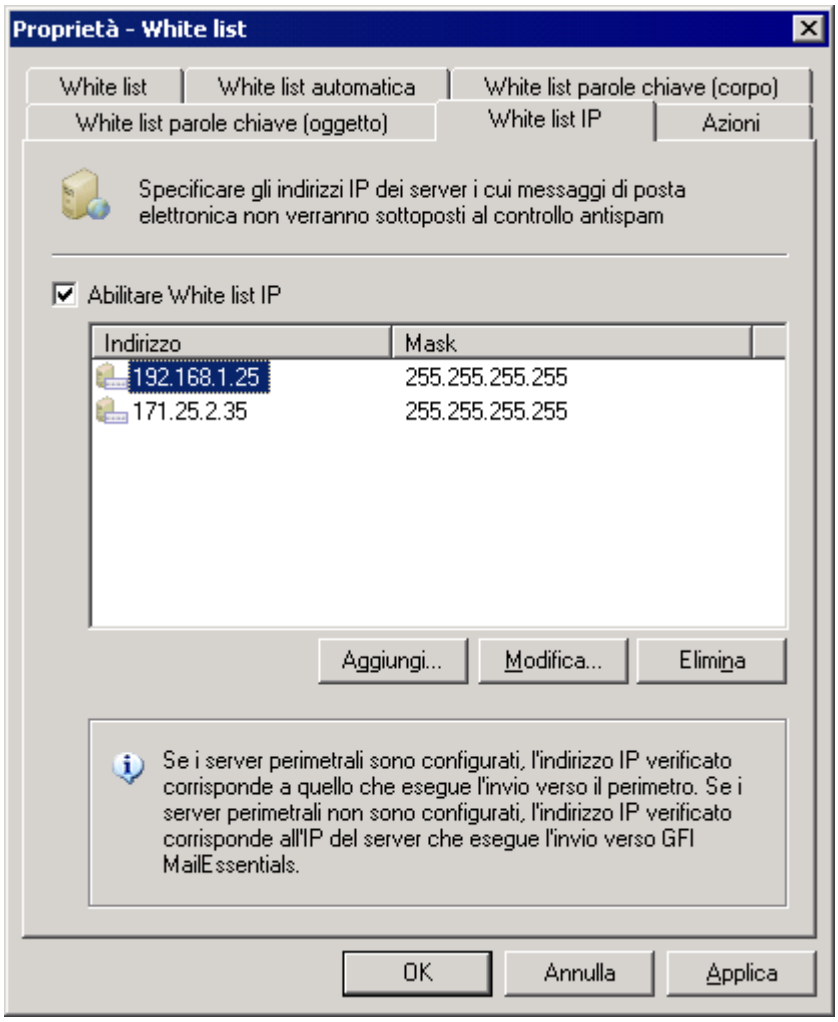
- **Popola la white list automatica in modo automatico:** selezionando questa opzione, gli indirizzi di posta elettronica di destinazione dei messaggi di posta elettronica in uscita sono aggiunti automaticamente alla white list
- **Numero massimo di voci consentite nella White list automatica:** specificare il numero di voci consentite nella White list automatica. Al superamento del limite specificato, le voci più vecchie vengono automaticamente sostituite con quelle nuove.
- **Abilita White list automatica di posta elettronica:** selezionando questa opzione i messaggi di posta elettronica in entrata sono sottoposti a scansione per confrontare i mittenti rispetto alla white list automatica. Se il mittente è presente nell'elenco, il messaggio di posta elettronica viene inoltrato direttamente alla Posta in arrivo del destinatario.

NOTA: è possibile visualizzare le voci della white list automatica nella scheda White list selezionando l'opzione **Mostra le voci inserite automaticamente** dal menu a discesa del **Filtro voci white list**.



Schermata 36 - Inserimento delle parole chiave nella white list

6. Selezionare le schede **Parole chiave inserite nella white list (Oggetto)** o **Parole chiave inserite nella white list (Corpo)** per specificare parole chiave intese a segnalare i messaggi di posta elettronica come ham (posta elettronica valida) e consentire automaticamente al messaggio di posta elettronica di evitare tutti i filtri antispam. Specificare nuove parole chiave facendo clic sul pulsante **Aggiungi** o usare i pulsanti **Rimuovi**, **Modifica**, **Importa** ed **Esporta** per modificare le parole chiave esistenti.



Schermata 37 - Inserimento di IP nella white list

7. Fare clic sulla scheda **White list di IP** per consentire automaticamente i messaggi di posta elettronica ricevuti da indirizzi IP specifici. Per abilitare questa caratteristica, selezionare l'opzione **Abilita white list IP** e fare clic sul pulsante **Aggiungi** per inserire un solo indirizzo IP o subnet/maschera per evitare i controlli antispam.

8. Fare clic sulla scheda **Azioni** per abilitare/disabilitare la registrazione di un'occorrenza white list in un file. Fare clic su **Sfoglia** per specificare una cartella dove salvare i registri.

9. Fare clic su **OK** per completare la configurazione.

4.2.6 Raccolta di directory

Gli attacchi di raccolta di directory si verificano quando uno spammer si serve di indirizzi di posta elettronica conosciuti per generare altri indirizzi di posta elettronica indirizzati a server di posta elettronica di aziende o di ISP. Questa tecnica consente allo spammer di inviare messaggi di posta elettronica a indirizzi di posta elettronica generati in maniera casuale. Alcuni di questi indirizzi corrispondono a utenti effettivi. Tuttavia, molti di loro sono indirizzi fasulli che intasano il server di posta dell'utente bersaglio.

GFI MailEssentials ferma questo tipo di attacchi bloccando i messaggi di posta elettronica indirizzati a utenti non presenti sull'Active Directory

o sul server di posta elettronica dell'organizzazione.

È possibile configurare l'esecuzione della raccolta di directory al ricevimento di un indirizzo di posta elettronica completo (*Transport sink*) o a livello di SMTP, ossia al ricevimento dell'IP di invio, di un messaggio di posta elettronica e dei destinatari (*SMTP protocol sink*). Il filtraggio a livello di SMTP conclude la connessione della posta elettronica arrestando di conseguenza lo scaricamento dell'indirizzo di posta elettronica completo, risparmiando in termini di ampiezza di banda ed elaborazione. In tal caso, la connessione termina immediatamente e i messaggi di posta elettronica non devono passare per altri filtri antispam.

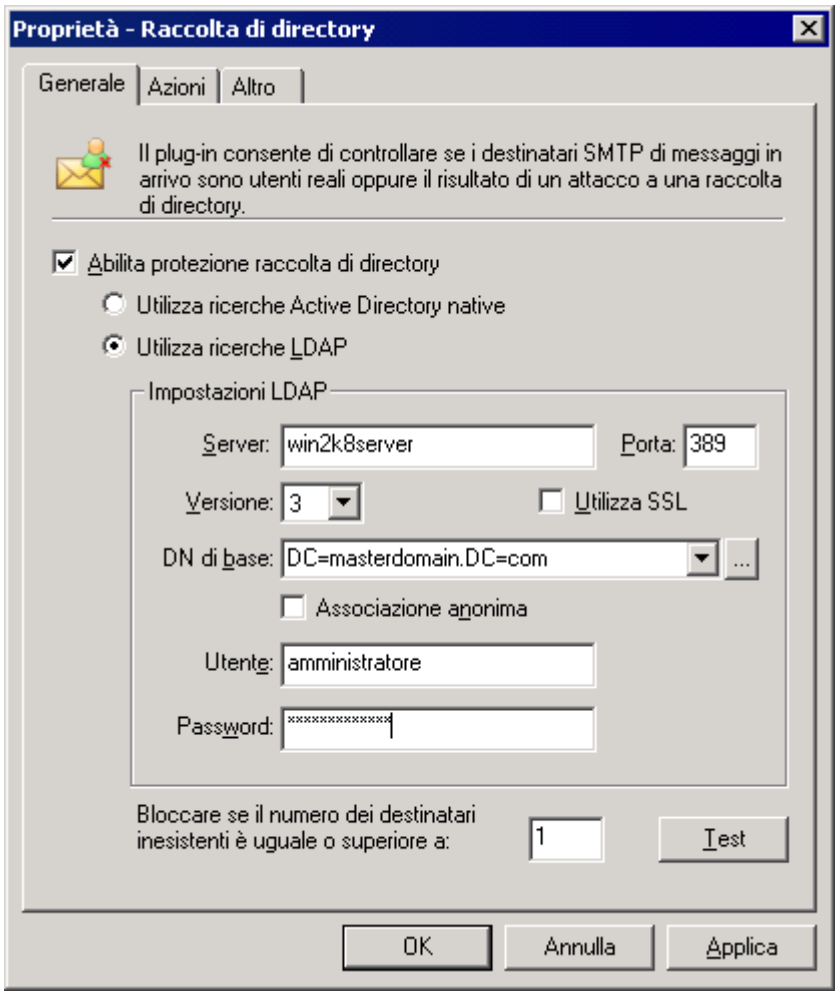
Questo filtro NON è abilitato per impostazione predefinita all'installazione di GFI MailEssentials.

Configurazione della raccolta di directory

La raccolta di directory viene configurata in due fasi:

Fase 1 - Configurazione delle proprietà della raccolta di directory

1. Selezionare **Antispam ► Filtri anitspam ► Raccolta di directory ► Proprietà** e fare clic sull'opzione **Abilita protezione raccolta di directory**.



Schermata 38 - La funzionalità della raccolta di directory

2. Selezionare il metodo delle ricerche per usare:

- l'opzione **Utilizza le ricerche Active Directory native** se GFI MailEssentials è installato in modalità utente di Active Directory.

  NOTA 1: se installato in modalità utente di Active Directory su una zona demilitarizzata (DMZ), GFI MailEssentials non comprende solitamente tutti gli utenti della rete (vale a dire, i destinatari dei messaggi di posta elettronica). In questo caso, si consiglia di eseguire i controlli di Raccolta di directory avvalendosi delle ricerche LDAP.

  NOTA 2: quando GFI MailEssentials è installato dietro un firewall, la funzionalità della Raccolta di directory non è in grado di collegarsi direttamente all'Active Directory interna a causa delle impostazioni del firewall. In tal caso, si devono utilizzare le ricerche LDAP per consentire il collegamento all'Active Directory interna della propria rete e accertarsi di abilitare la porta predefinita 389 sul proprio firewall.

- Se GFI MailEssentials è installato in modalità SMTP, si devono **utilizzare le ricerche LDAP** per configurare le proprie impostazioni LDAP. Se il server LDAP in uso richiede l'autenticazione, deselezionare l'opzione **Collegamento anonimo** e inserire i dati di autenticazione che saranno utilizzati da tale funzionalità. Fare clic sul pulsante **Prova** per provare le impostazioni di configurazione LDAP.

  NOTA 1: indicare le credenziali di autenticazione usando la forma Dominio\Utente (per esempio, master-domain\administrator).

  NOTA 2: in un'Active Directory, normalmente, il server LDAP rappresenta in genere il controller di dominio.

3. Nell'opzione **Blocca se il numero dei destinatari inesistenti è uguale o superiore a** specificare il numero di destinatari non esistenti per qualificare il messaggio di posta elettronica come SPAM. Se il numero complessivo di destinatari è inferiore alla soglia, l'azione configurata viene attivata unicamente se TUTTI i destinatari non esistono, altrimenti il messaggio di posta elettronica non è contrassegnato come SPAM.

NOTA: per evitare di ottenere troppi falsi positivi, si consiglia di impostare un valore ragionevole nella casella **Blocca se il numero dei destinatari inesistenti è uguale o superiore a.** Va infatti considerato che, a volte, gli utenti inviano messaggi di posta elettronica legittimi digitando erroneamente gli indirizzi di posta elettronica oppure li inviano a utenti che non sono più dipendenti dell'azienda.

4. Fare clic sulla scheda **Azioni** o **Altro** per selezionare le azioni da eseguire sui messaggi individuati come spam. Per maggiori informazioni sulle azioni da intraprendere, consultare la sezione Azioni antispam: cosa fare dei messaggi di spam a pagina 73 del presente manuale.

NOTA: se la raccolta di directory è impostata al livello dell'*SMTP protocol sink*, sarà disponibile solamente l'opzione **Registra occorrenza** nella scheda **Azioni**.

Fase 2 - Selezione del metodo della raccolta di directory

1. Andare su **Antispam ► Priorità filtro ► Proprietà** e fare clic sul nodo **Filtraggio trasmissione SMTP**.

Schermata 7- Finestra di dialogo per l'ordine antispam

2. Fare clic sul pulsante per passare da/a:

- **Passa al filtraggio completo della posta elettronica** - il filtraggio viene eseguito al ricevimento di tutta la posta elettronica.
- **Passa al filtraggio trasmissione SMTP** - il filtraggio viene eseguito durante la trasmissione SMTP verificando l'esistenza dei destinatari del messaggio di posta elettronica prima del ricevimento del corpo del messaggio e degli allegati.

  NOTA: scegliendo questa opzione la Raccolta di directory sarà eseguita sempre prima di altri filtri antispam.

3. Fare clic su **OK** per completare la configurazione.

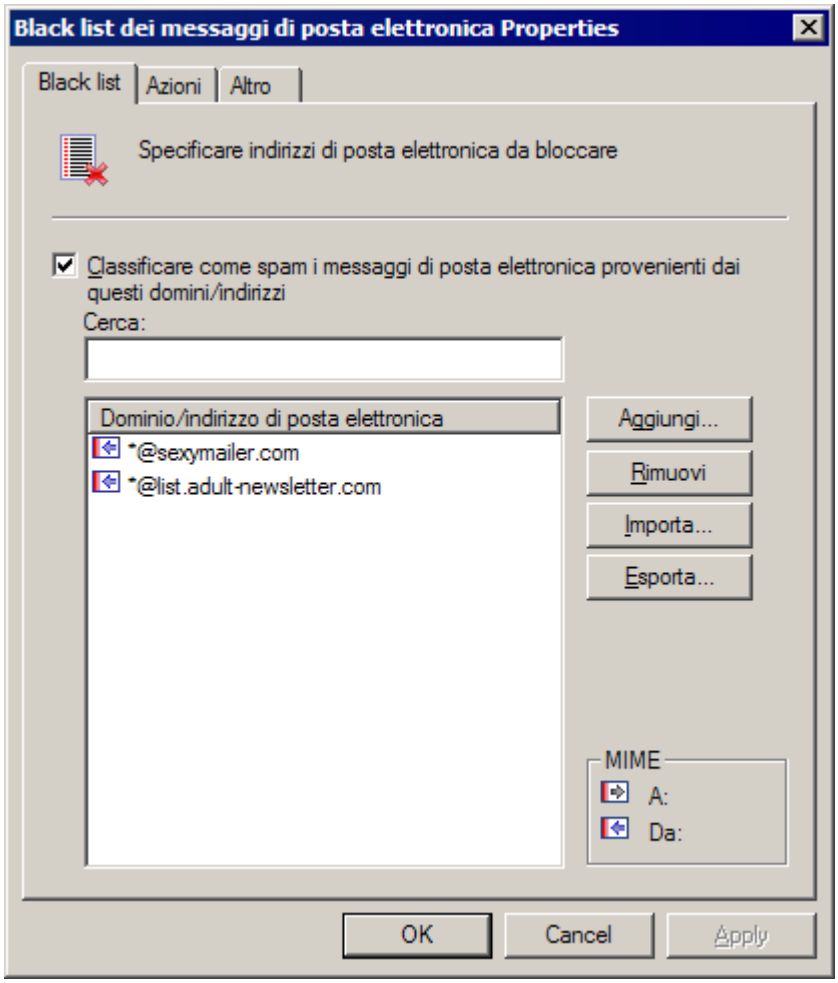
4.2.7 Black list dei messaggi di posta elettronica

La black list è un data base personalizzato di indirizzi di posta elettronica e domini da cui non si desidera mai ricevere la posta elettronica.

Questo filtro è abilitato per impostazione predefinita all'installazione di GFI MailEssentials.

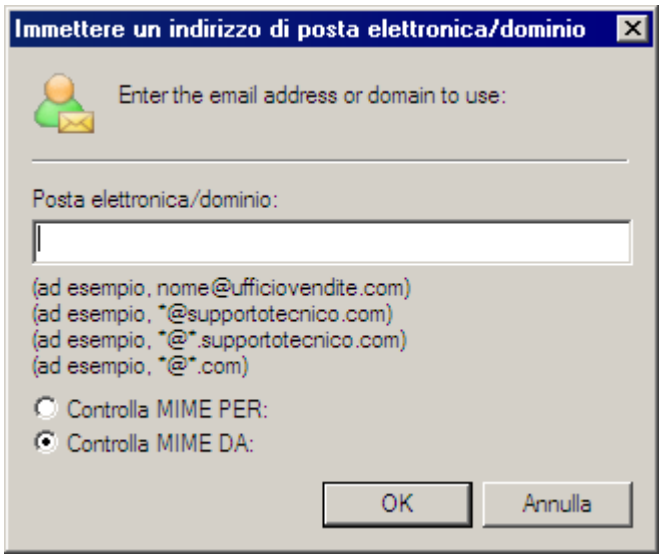
Configurazione personalizzata delle black list

Selezionare **Antispam ► Filtri antispam ► Black list dei messaggi di posta elettronica ► Proprietà.**



Schermata 8 - La black list di URI anti-spam in temp reale

2. Fare clic su **Aggiungi** per aggiungere un dominio o un indirizzo di posta elettronica nella black list.



Schermata 41 - Aggiunta di un indirizzo di posta elettronica alla black list

3. Nella finestra di dialogo **Immettere un indirizzo di posta elettronica/dominio** indicare l'indirizzo di posta elettronica completo o un intero dominio (per esempio: *@spammer.com); o il suffisso di un intero dominio (per esempio: *@*.tv). Per indicare inoltre a quale campo dell'intestazione del messaggio di posta elettronica deve corrispondere tale voce, in modo da poter inserire il messaggio in questione nella black list, fare clic su **Controlla MIME PER:** o **Controlla MIME DA:**

4. Per ricercare indirizzi di posta elettronica e domini nella black list, digitare un criterio di ricerca nella casella di testo di **Ricerca**. Le voci corrispondenti saranno automaticamente visualizzate sotto.

5. Selezionare la scheda **Azioni** o **Altro** per selezionare le azioni da eseguire sullo spam. Per maggiori informazioni, consultare la sezione Azioni antispam: cosa fare dei messaggi di spam a pagina 73 del presente manuale.

6. Fare clic su **OK** per completare la configurazione.

4.2.8 Analisi bayesiana

Il filtro bayesiano costituisce una tecnologia antispam di GFI MailEssentials che impiega tecniche adattive basate su algoritmi di intelligenza artificiale, resi più rigorose per far fronte alla più estesa serie di tecniche di spam disponibili oggi.

Per maggiori informazioni sulla modalità di funzionamento, configurazione e addestramento del filtro bayesiano, consultare Appendice 2 Filtraggio bayesiano a pagina 139 del presente manuale.

NOTA: il filtro antispam bayesiano è disabilitato per impostazione predefinita.

IMPORTANTE: Attendere almeno una settimana perchè il filtro bayesiano raggiunga le massime prestazioni dopo la sua abilitazione. Il filtro bayesiano raggiunge la più alta percentuale d'individuazione dello spam adattandosi in maniera specifica ai modelli di posta elettronica dell'utente.

Configurazione del filtro bayesiano

La configurazione del filtro bayesiano si svolge in 2 fasi:

Fase 1: Addestramento del filtro bayesiano

Fase 2: Abilitazione del filtro bayesiano

Fase 1: Addestramento del filtro bayesiano

Il filtro bayesiano può essere addestrato in due modi:

1. Automaticamente, attraverso i messaggi di posta elettronica in uscita.

GFI MailEssentials raccoglie messaggi di posta elettronica legittimi (ham) eseguendo la scansione di messaggi in uscita. Il filtro bayesiano può essere abilitato dopo che ha raccolto almeno 500 messaggi di posta elettronica in uscita (se si inviano principalmente messaggi in inglese) o 1.000 messaggi di posta elettronica in uscita (se si inviano messaggi in una lingua diversa dall'inglese).

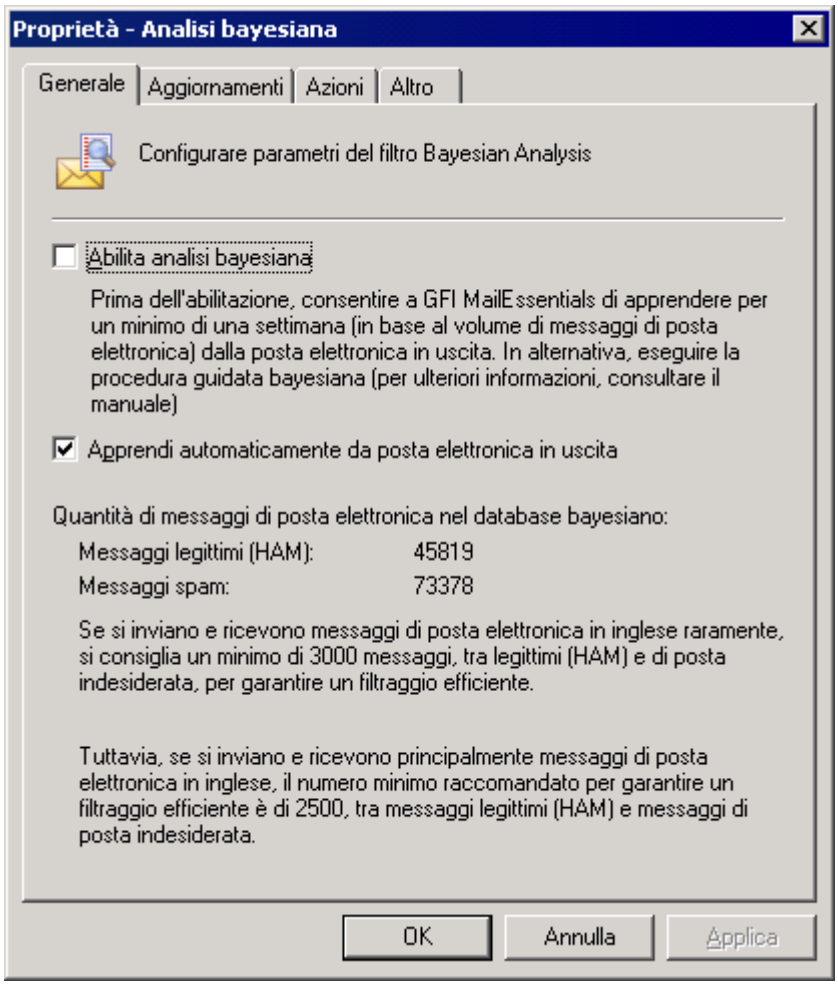
Schermata 42 - Fornitura di ham al filtro bayesiano

2. Manualmente, attraverso la posta elettronica esistente.

Copiando tra 500 e 1.000 messaggi dalla posta inviata nella sottocartella **Messaggio legittimo** nelle cartelle pubbliche **Cartelle anti-spam GFI** si addestra il filtro bayesiano come quando vengono inviati i messaggi di posta elettronica in tempo reale.

Fase 2: Abilitazione del filtro bayesiano

Dopo che è addestrato, il filtro bayesiano deve essere abilitato.



Schermata 43 - Proprietà dell' analisi bayesiana

1. Dalla console di GFI MailEssentials configuration, selezionare **Antispam ► Filtri antispam ► Analisi bayesiana ► Proprietà**. Dalla scheda **Generale**, selezionare la casella di controllo **Abilita analisi bayesiana**.

2. Accertarsi che sia abilitata l'opzione **Apprendi automaticamente da posta elettronica in uscita**. Questa opzione aggiorna costantemente il data base di messaggi di posta elettronica legittimi con i dati dei messaggi di posta elettronica in uscita.

3. Nella scheda **Aggiornamenti**, configurare la frequenza degli aggiornamenti nel data base dello spam abilitando **Verifica automaticamente gli aggiornamenti** e configurando un intervallo orario.

NOTA 1: fare clic sul pulsante **Scarica aggiornamenti adesso**… per scaricare immediatamente gli aggiornamenti.

NOTA 2: Per maggiori informazioni su come selezionare i server preferiti e come scaricare gli aggiornamenti con un server proxy consultare Configurazione aggiornamenti automatici a pagina 116 di questo manuale.

4. Fare clic sulla scheda **Azioni** o **Altro** per selezionare le azioni da eseguire sui messaggi individuati come spam. Per maggiori informazioni sulle azioni da intraprendere, consultare la sezione Azioni antispam: cosa fare dei messaggi di spam a pagina 73 del presente manuale.

5. Fare clic su **OK** per completare la configurazione.

4.2.9 Black list DNS (DNSBL)

GFI MailEssentials supporta alcune black list DNS. Le black list DNS sono data base di server SMTP utilizzati ai fini dello spam. Sono disponibili numerose black list DNS di terzi, che variano da elenchi affidabili, che definiscono con chiarezza le procedure per aggiungere o rimuovere la black list DNS, a elenchi meno affidabili.

Quando si invia un messaggio di posta elettronica, questo attraversa un certo numero di server SMTP fino a raggiungere la propria destinazione finale. L'indirizzo IP di ciascuno di questi server SMTP è registrato nell'intestazione (header) del messaggio di posta elettronica. GFI MailEssentials confronta tutti gli indirizzi IP pubblici trovati nell'intestazione del messaggio con il data base DNSBL configurato.

GFI MailEssentials registra tutti gli indirizzi IP confrontati in un data base interno e non esegue ulteriori confronti con il DNSBL per gli stessi indirizzi. Gli indirizzi IP sono conservati nel data base per 4 giorni oppure fino a quando non viene riavviato il servizio SMTP (*Simple Mail Transport Protocol*).

Questo filtro è abilitato per impostazione predefinita all'installazione di GFI MailEssentials.

Note importanti

1. Il server DNS deve essere correttamente configurato per il funzionamento di questa caratteristica. In caso contrario, si verificheranno dei timeout e il traffico di posta elettronica verrà rallentato leggermente. Consultare http://kbase.gfi.com/showarticle.asp?id=KBID001770 per maggiori informazioni.

2. L'interrogazione di una black list DNS può essere lenta (dipende dal tipo di connessione utilizzato); pertanto il messaggio di posta

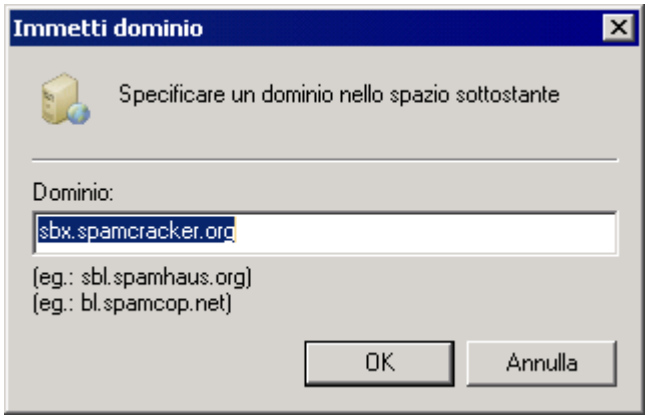
elettronica può essere scaricato un po' più lentamente, soprattutto se si interrogano più black list DNS.

Configurazione di DNSBL

1. Selezionare **Antispam ► Filtri antispam ► Black list DNS ► Proprietà.**

2. Selezionare la casella di controllo **Controllare se il server di invio posta è presente in una delle seguenti black list DNS** :

3. Selezionare la black list DNS che si desidera confrontare con i messaggi di posta elettronica in entrata e fare clic sul pulsante **Prova** per verificare la disponibilità delle black list selezionate.



Schermata 44 - Aggiunta di più black list DNS

4. È inoltre possibile aggiungere altre black list DNS a quelle già elencate, facendo clic sul pulsante **Aggiungi** e inserire il dominio contenente la DNSBL.

NOTA: per modificare l'ordine di riferimento di una black list DNS abilitata, selezionare la black list interessata e quindi fare clic sui pulsanti **Su** o **Giù**.

5. Selezionare **Bloccare i messaggi inviati da indirizzi IP dinamici elencati in SORBS.net** per abilitare GFI MailEssentials a rilevare spam inviati da botnet/zombie cercando l'IP di connessione in entrata con gli indirizzi IP botnet/zombie noti nel data base Sorbs.net.

6. Fare clic su **Applica** per salvare la configurazione.

Schermata 45 - Configurazione dell'attuale server SMTP perimetrale

7. Se questo computer **NON** costituisce il server SMTP perimetrale, compare una finestra di dialogo che mostra le impostazioni di SMTP perimetrale precedentemente configurate in GFI MailEssentials (cioè gli indirizzi IP specificati per il proprio server SMTP perimetrale).

Schermata 46 - Promemoria: Sender Policy Framework deve essere installato sul server SMTP perimetrale

7. Se GFI MailEssentials è installato sul server SMTP o se non si è ancora indicato il server di posta su cui il prodotto è installato, compare una finestra di dialogo di notifica che indica che il computer in uso non è un server perimetrale.

8. Fare clic sulla scheda **Azioni** o **Altro** per selezionare le azioni da eseguire sui messaggi individuati come spam. Per maggiori informazioni sulle azioni da intraprendere, consultare la sezione sezione Azioni antispam: cosa fare dei messaggi di spam a pagina 73 del presente manuale.

9. Fare clic su **OK** per completare la configurazione.

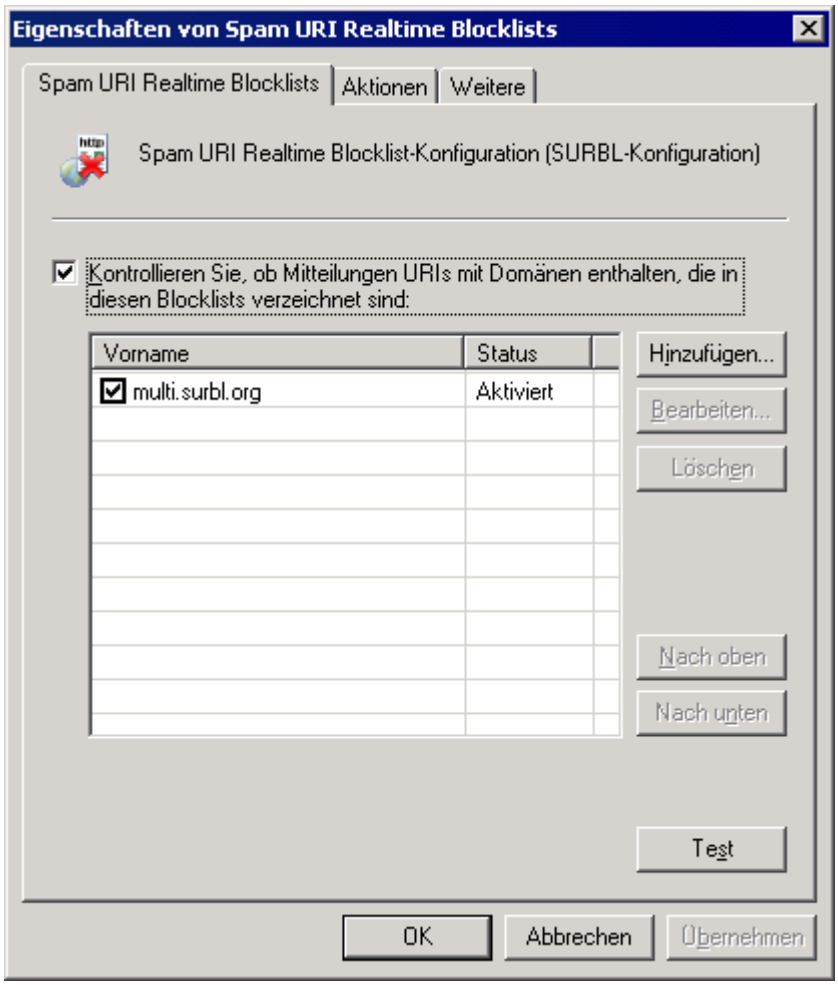
4.2.10 Blocklist di URI antispam in tempo reale (SURBL)

Un URI (Universal Resource Identifier, Identificatore Universale di Risorse) rappresenta un mezzo standard di indirizzamento delle risorse sul Web. URI comuni, quali *Uniform Resource Locators* (URL) e *Universal Resource Names* (URN) sono utilizzati per identificare la destinazione di collegamenti ipertestuali e le sorgenti di immagini, informazioni e altri oggetti di una pagina Web. Gli URL sono perlopiù utilizzati in siti Web, ma possono anche essere inclusi nel corpo di un messaggio di posta elettronica.

Le Block list di URI anti-spam in tempo reale si differenziano dalla maggior parte delle RBL in quanto sono utilizzate per individuare lo spam basato su URI nel corpo del messaggio. A differenza di molte altre RBL, le SURBL non sono utilizzate per bloccare i mittenti di spam. Consentono invece di bloccare i messaggi che hanno *spam-host* (per esempio: server Web, domini, siti Web) menzionati nel corpo del messaggio.

Questo filtro è abilitato per impostazione predefinita all'installazione di GFI MailEssentials.

Configurazione delle Block list di URI anti-spam in tempo reale



Schermata 47 - Proprietà della black list di URI antispam in tempo reale

1. Selezionare **Antispam ► Filtri Antispam ► Blocklist di URI anti-spam in tempo reale ► Proprietà.**

2. Dalla scheda Black list di URI antispam in tempo reale:

- Selezionare/deselezionare l'opzione **Controllare se i messaggi di posta elettronica contengono URI i cui domini sono presenti nelle seguenti black list:** per abilitare/disabilitare questa funzionalità.
- Nell'elenco fornito, selezionare le black list da utilizzare come riferimento quando si controllano i messaggi con la funzione SURBL.
- Fare clic sul pulsante **Aggiungi** per aggiungere più SURBL.

Eseguire la prova di connessione facendo clic sul pulsante **Prova** e su **Applica** per salvare le configurazioni.

NOTA 1: indicare il nome completo del dominio (per esempio URIBL.com) contenente la black list.

NOTA 2: Multi.surbl.org combina in un unico elenco le seguenti liste:

- sc.surbl.org
- ws.surbl.org

- la sorgente di dati phishing da “mailsecurity.net.au”
- la sorgente di dati phishing da “fraud.rhs.mailpolice.com”
- ob.surbl.org
- ab.surbl.org
- jp data source

Quando si abilita “multi.surbl.org”, si consiglia di disabilitare tutte le altre liste Block list di URI anti-spam in tempo reale dalla configurazione in quanto potrebbero aumentare i tempi di elaborazione della posta elettronica.

Se Block list di URI anti-spam in tempo reale produce molti falsi positivi, si consiglia di disabilitare “multi.surbl.org” e abilitare le altre liste.

Per maggiori informazioni sulle liste Block list di URI anti-spam in tempo reale, consultare http://www.surbl.org/lists.html.

5. Fare clic sulla scheda **Azioni** o **Altro** per selezionare le azioni da eseguire sui messaggi individuati come spam. Per maggiori informazioni sulle azioni da intraprendere, consultare la sezione Azioni antispam: cosa fare dei messaggi di spam a pagina 73 del presente manuale.

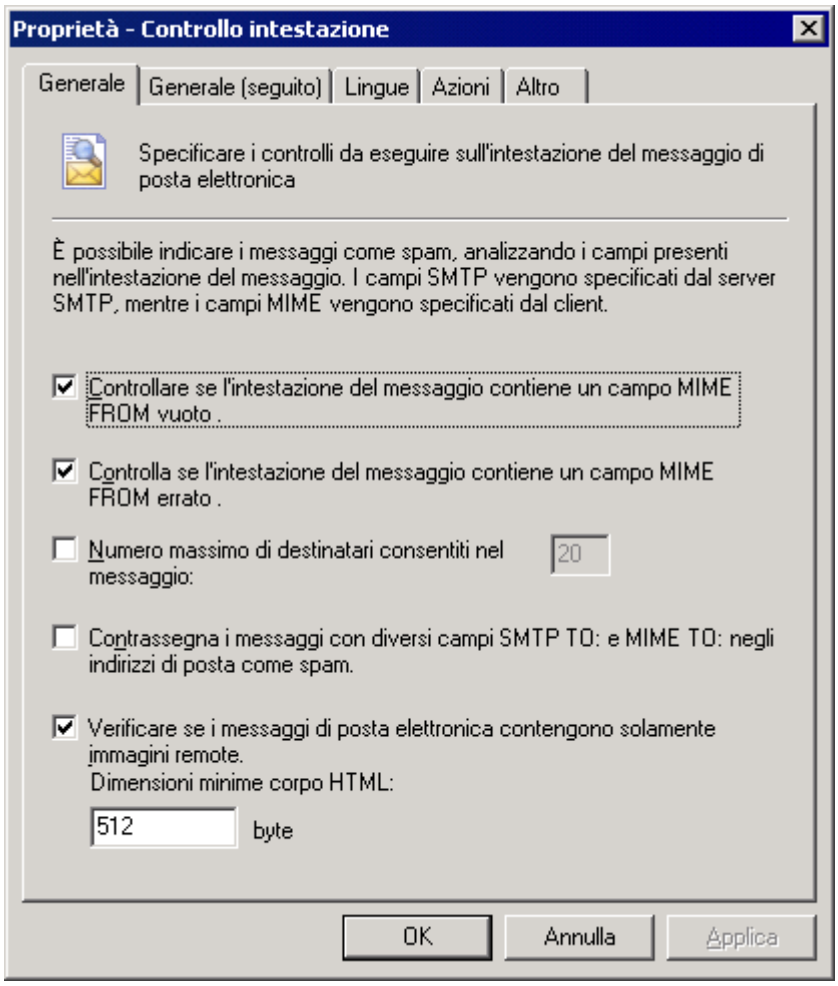
6. Fare clic su **OK** per completare la configurazione.

4.2.11 Controllo intestazioni

Il modulo di controllo intestazioni analizza i singoli campi di un’intestazione. Questo modulo fa riferimento ai campi SMTP e MIME. I campi SMTP sono specificati dal server di posta, mentre i campi MIME sono specificati dal client di posta elettronica (che codifica la posta elettronica su MIME).

Configurazione del controllo delle intestazioni

1. Selezionare **Antispam ► Filtri antispam ► Controllo intestazioni ► Proprietà.**



Schermata 48 - Scheda generale del controllo delle intestazioni

2. Nelle schede **Generale** e **Generale Contd.** è possibile abilitare, disabilitare o configurare i seguenti parametri:

- **Controlla se l'intestazione del messaggio di posta contiene un campo MIME FROM vuoto:** questa caratteristica verifica se il mittente ha identificato se stesso nel campo *From:* (Da:) . Se tale campo è vuoto il messaggio è contrassegnato come spam.
- **Controlla se l'intestazione del messaggio contiene un campo MIME FROM errato :** questa caratteristica verifica se il campo "MIME Da:" è corretto, ossia, se l'intestazione corrisponde all'RFC.
- **Numero massimo di destinatari consentiti nel messaggio:** questa caratteristica identifica e contrassegna come spam i messaggi di posta elettronica contenenti lunghi elenchi di destinatari.
- **Contrassegna i messaggi di posta con diversi campi SMTP TO: e MIME TO: negli indirizzi di posta elettronica come spam:** verifica se i campi *SMTP to:* (SMTP A:) e "MIME to:" (MIME A:) sono gli stessi. Il server di posta degli spammer deve sempre contenere un indirizzo *SMTP to:* (SMTP A:) . Tuttavia, l'indirizzo di posta elettronica *MIME to:* (MIME A:) spesso non è incluso oppure è diverso.

  NOTA: questa caratteristica permette di catturare molto spam; tuttavia, anche alcuni server di elenco non comprendono il campo

MIME to: (MIME A:) . Pertanto, per utilizzare tale caratteristica, si deve inserire l'indirizzo del mittente della newsletter nella white list, nel caso fosse contrassegnato come spam dalla suddetta caratteristica.

- **Controllare se i messaggi contengono solamente immagini remote:** contrassegna come spam i messaggi di posta elettronica contenenti solo immagini remote e una quantità minima di testo. Assiste nell'individuazione di messaggi di spam di solo immagini.
- **Verificare se il dominio del mittente è valido:** esegue una ricerca DNS sul dominio specificato nel campo *MIME from* (MIME Da) e ne verifica la validità.

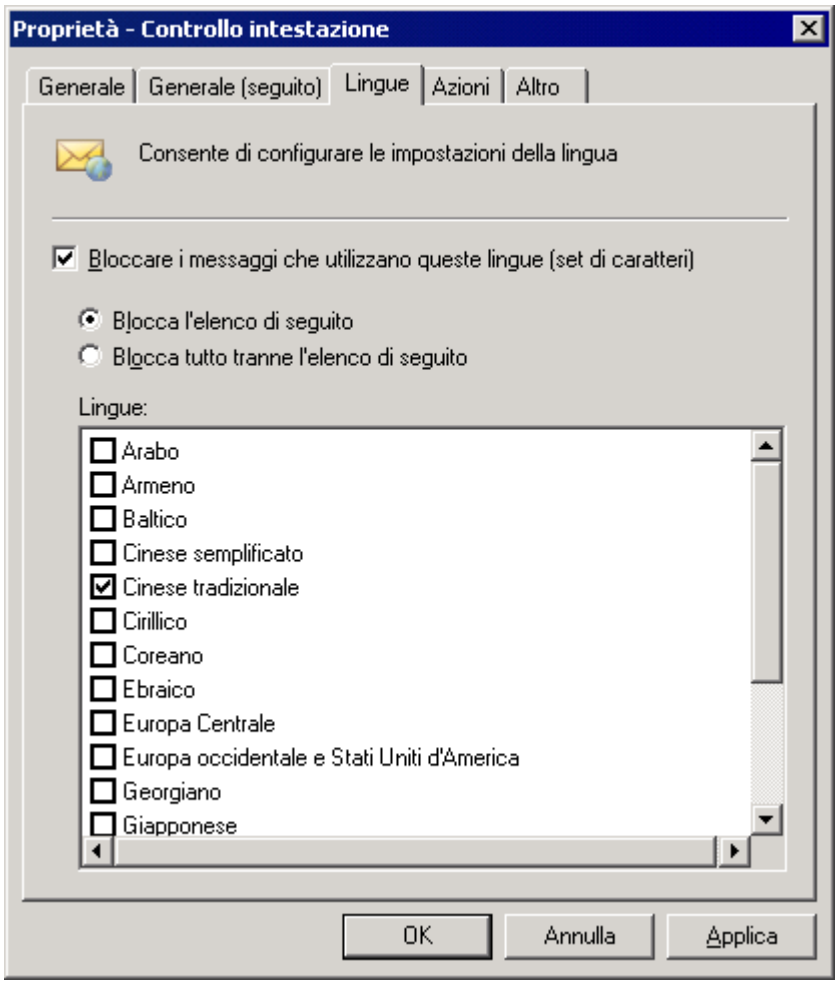
  NOTA: questa caratteristica richiede un server DNS opportunamente configurato; diversamente, si verifica un timeout e i messaggi di posta elettronica vengono elaborati lentamente. Inoltre, molti messaggi di posta elettronica validi saranno etichettati come spam. È possibile provare i propri servizi o server DNS facendo clic sul pulsante **Prova**.
- **Numero massimo di numeri consentiti in MIME FROM:** la presenza di più di tre numeri nel campo "MIME Da:" indica che ci troviamo di fronte a un messaggio di spam. Questo perché gli spammer si avvalgono spesso di strumenti per creare automaticamente indirizzi "*reply-to:*" ("rispondi a:"). Utilizzano di solito 3 o più numeri all'interno del nome per assicurarsi che l'indirizzo "*reply-to:* (rispondi a:) sia esclusivo.
- **Controlla se l'oggetto del messaggio contiene la prima parte dell'indirizzo di posta del destinatario:** individua un messaggio di spam personalizzato dove gli spammer spesso immettono la prima parte dell'indirizzo di posta elettronica del destinatario nell'oggetto.

  NOTA: è possibile indicare gli indirizzi di posta elettronica per i quali tale controllo non deve essere eseguito, facendo clic sul pulsante **Esclusi…**. Tale azione abilita gli indirizzi di posta elettronica generici con cui rispondono i clienti, per esempio messaggi di posta elettronica da sales@company.com aventi come oggetto "Il Suo messaggio all'ufficio vendite", a non essere contrassegnati come spam.
- **Controllare se il messaggio contiene indirizzi IP codificati:** controlla l'intestazione e il corpo del messaggio per URL che contengano IP esadecimali/ottali codificati (http://0072389472/hello.com) o una combinazione del tipo nome utente/password (per esempio, www.citibank.com@scammer.com).
  - Esempi di messaggi di posta elettronica che saranno contrassegnati come spam:
    - *http://12312*
    - *www.microsoft.com:hello%01@123123*
- **Controllare se il messaggio contiene immagini GIF incorporate:** controlla se il messaggio contiene una o più immagini GIF incorporate. Le immagini GIF incorporate sono spesso usate per aggirare i filtri antispam.

  IMPORTANTE: Dal momento che i messaggi di posta

elettronica legittimi contengono immagini GIF incorporate, tale opzione è soggetta ai falsi positivi.

- **Controllare se il messaggio contiene allegati spam:** controlla le proprietà degli allegati dei messaggi di posta elettronica comuni agli allegati inviati nei messaggi di spam. Tale azione consente di stare al passo con le ultime tecniche adoperate degli spammer nell'invio di allegati per diffondere messaggi di spam.



Schermata 49 - Rilevamento della lingua

3. Nella scheda Lingua, selezionare l'opzione **Bloccare i messaggi che utilizzano queste lingue (set di caratteri)** per bloccare i messaggi di posta elettronica inviati usando set di caratteri non comuni ai messaggi di posta elettronica ricevuti (per esempio cinese e vietnamita).

NOTA: questa funzionalità non riesce a distinguere, per esempio, tra francese e italiano perché tali lingue utilizzano lo stesso set di caratteri.

4. Fare clic sulla scheda **Azioni** o **Altro** per selezionare le azioni da eseguire sui messaggi individuati come spam. Per maggiori informazioni sulle azioni da intraprendere, consultare la sezione Azioni antispam: cosa fare dei messaggi di spam a pagina 73 del presente manuale.

5. Fare clic su **OK** per completare la configurazione.

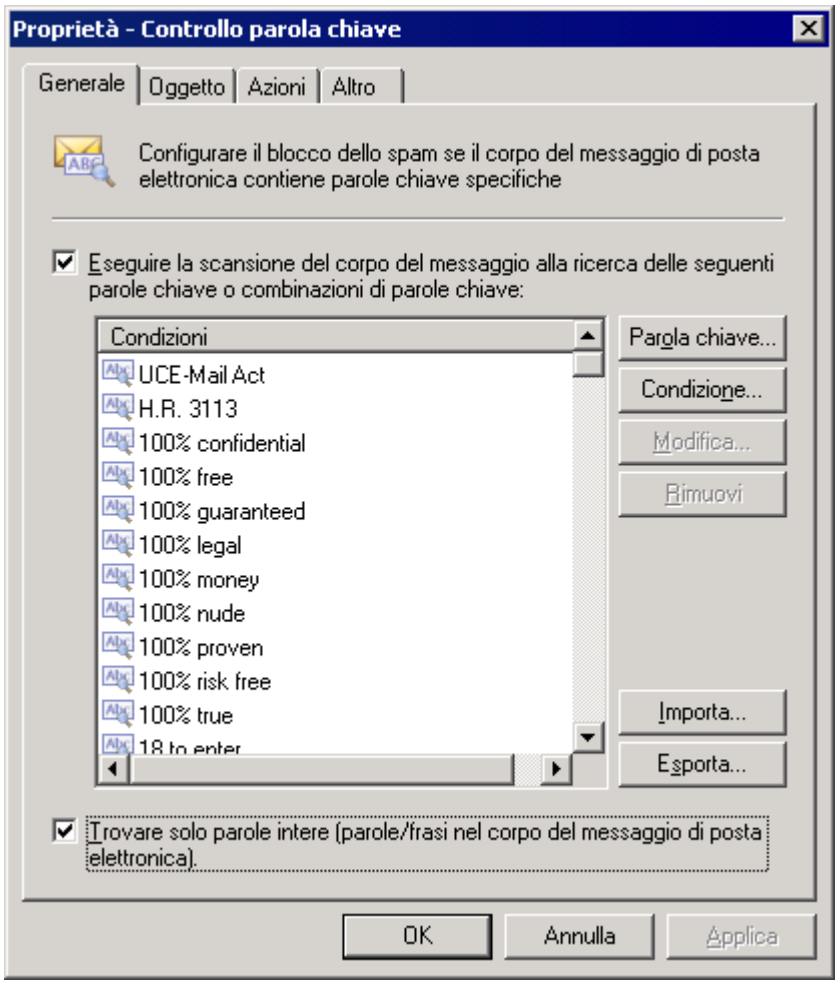
4.2.12 Controllo parole chiave

Il controllo parole chiave abilita l'individuazione di messaggi di spam sulla base di parole chiave nel messaggio di posta elettronica ricevuto.

Questo filtro NON è abilitato per impostazione predefinita.

Configurazione del controllo parole chiave

1. Selezionare **Antispam ► Filtri antispam ► Controllo parole chiave ► Proprietà.**

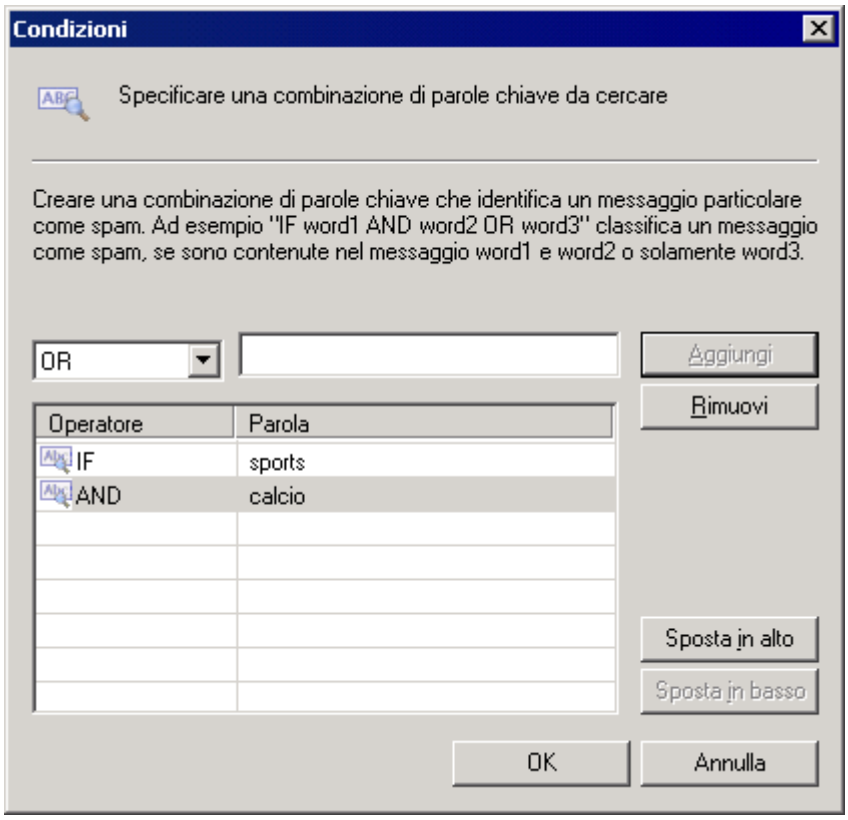


Schermata 50 - Proprietà del controllo antispam parole chiave

2. Scegliere la casella di controllo Eseguire la scansione del corpo del messaggio alla ricerca delle seguenti parole chiave o combinazioni di parole chiave: per abilitare questa funzionalità.

3. Fare clic sul pulsante **Parola chiave** per inserire le parole chiave. Se vengono inserite parole multiple, GFI MailEssentials cerca quella frase.

- **Esempio:** Per "Sport basketball", GFI MailEssentials controllerà la frase "Sport basketball". Solamente questa frase attiverà la regola, non la parola basketball o sport separate da altre parole.



Schermata 51 - Aggiunta di una condizione

4. Aggiungere gli operatori logici facendo clic sul pulsante **Condizione…**

NOTA: le condizioni sono combinazioni di parole chiave che utilizzano gli operandi *IF, AND, AND NOT, OR, OR NOT*. L'utilizzo di condizioni permette di specificare combinazioni di parole che devono comparire nel messaggio di posta elettronica.

- **Esempio:** la condizione "If Parola1 AND Parola2" cercherà sia la Parola1 sia la Parola2. Per abilitare la regola, entrambe le parole devono essere presenti nel messaggio di posta elettronica.

Per aggiungere una condizione, fare clic sul pulsante **Condizione…**

5. Scegliere la scheda **Oggetto** e selezionare la casella di controllo **Eseguire la scansione dell'oggetto del messaggio alla ricerca delle seguenti parole chiave o combinazioni di parole chiave.** È quindi possibile specificare le parole che si desidera ricercare nell'oggetto del messaggio.

- Per inserire parole o frasi singole senza operatori logici, fare clic sul pulsante **Parola chiave…**
- Per inserire parole chiave combinate con operatori logici, fare clic sul pulsante **Condizione…**

6. Fare clic sulla scheda **Azioni** o **Altro** per selezionare le azioni da eseguire sui messaggi individuati come spam. Per maggiori informazioni sulle azioni da intraprendere, consultare la sezione sezione Azioni antispam: cosa fare dei messaggi di spam a pagina 73 del presente manuale.

7. Fare clic su **OK** per completare la configurazione.

4.2.13 Filtro nuovi mittenti

Grazie al filtro nuovi mittenti, GFI MailEssentials è in grado di identificare automaticamente messaggi di posta elettronica inviati da mittenti cui l'utente non ha mai inviato messaggi di posta elettronica prima d'ora. Tali mittenti sono identificati facendo riferimento ai dati raccolti nelle white list.

Nella cartella Nuovi mittenti, vengono recapitati unicamente i messaggi di posta elettronica in cui non si è individuato spam e i cui mittenti non sono presenti in nessuna white list.

Poiché possono essere stati inviati da utenti legittimi, tali messaggi di posta elettronica vengono raccolti in una cartella dedicata. Ciò li rende facilmente identificabili. Successivamente, è possibile rivedere i messaggi di posta elettronica e aggiungere alla black list personale l'eventuale spam non identificato.

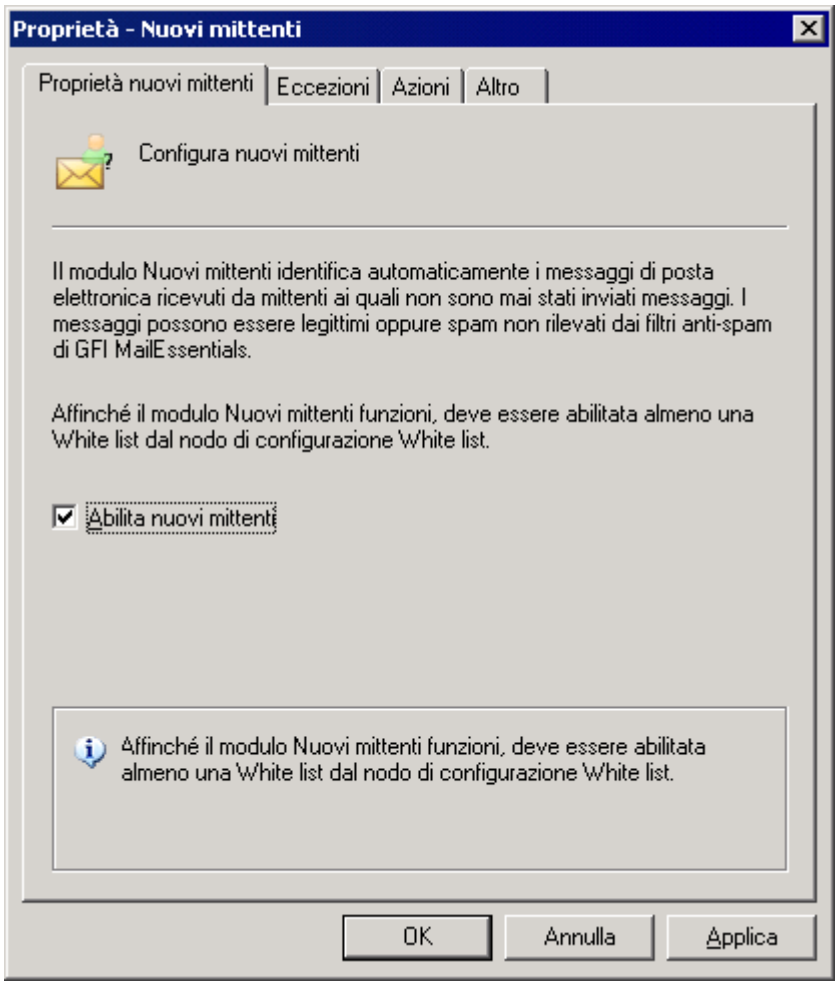
Questo filtro NON è abilitato per impostazione predefinita.

Note importanti

1. È necessario abilitare almeno una delle White list disponibili per poter utilizzare la funzione Nuovi mittenti. In assenza di funzioni White list (nel caso non venga individuato alcuno spam dagli altri filtri), i messaggi ricevuti vengono recapitati nella Posta in arrivo del destinatario. Nella cartella Nuovi mittenti, vengono recapitati **UNICAMENTE** i messaggi di posta elettronica in cui non si è individuato spam e i cui mittenti non sono presenti in nessuna white list.

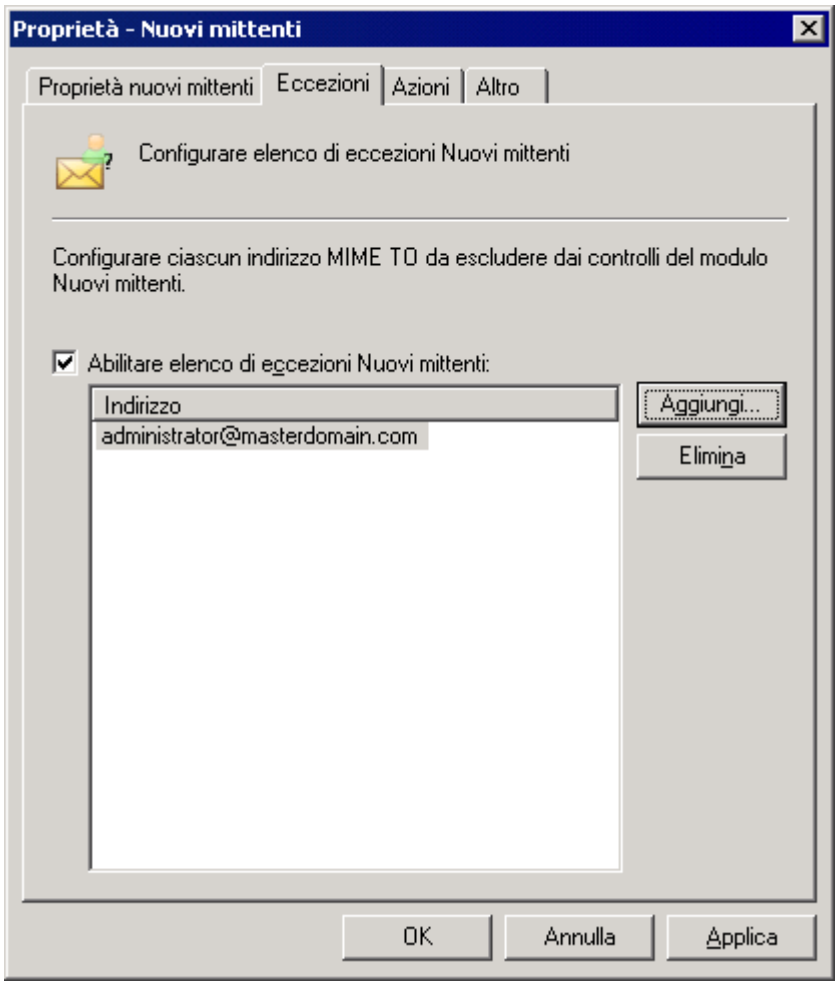
Configurazione del filtro Nuovi mittenti

1. Selezionare **Antispam ► Nuovi mittenti ► Proprietà.**



Schermata 52 - Proprietà della cartella Nuovi mittenti

2. Nella scheda **Proprietà Nuovi mittenti**, selezionare la casella di controllo **Abilita Nuovi mittenti** per abilitare la ricerca di nuovi mittenti in tutti i messaggi in arrivo e fare clic sul pulsante **Applica**.



Schermata 53 - Configurazione delle eccezioni per Nuovi mittenti

3. Selezionare la scheda **Eccezioni** e selezionare la casella di controllo **Elenco eccezioni MIME TO:** per configurare i destinatari locali i cui messaggi di posta elettronica devono essere esclusi dal controllo Nuovi mittenti.

4. Fare clic sul pulsante **Aggiungi…** e inserire l'indirizzo di posta elettronica del mittente.

- **Esempio:** administrator@master-domain.com.

Ripetere la stessa procedura per ogni indirizzo da aggiungere e fare poi clic sul pulsante **Applica** per salvare.

NOTA: se si desidera disabilitare temporaneamente l'elenco delle eccezioni, non è necessario eliminare tutte le voci di indirizzo immesse, ma è sufficiente deselezionare la casella di **Elenco eccezioni MIME TO** :

5. Fare clic sulla scheda **Azioni** per selezionare le azioni da eseguire sui messaggi individuati come spam. Per maggiori informazioni sulle azioni da intraprendere, consultare la sezione Azioni antispam: cosa fare dei messaggi di spam a pagina 73 del presente manuale.

6. Fare clic su **OK** per completare la configurazione.

4.2.14 Azioni antispam: cosa fare dei messaggi di spam

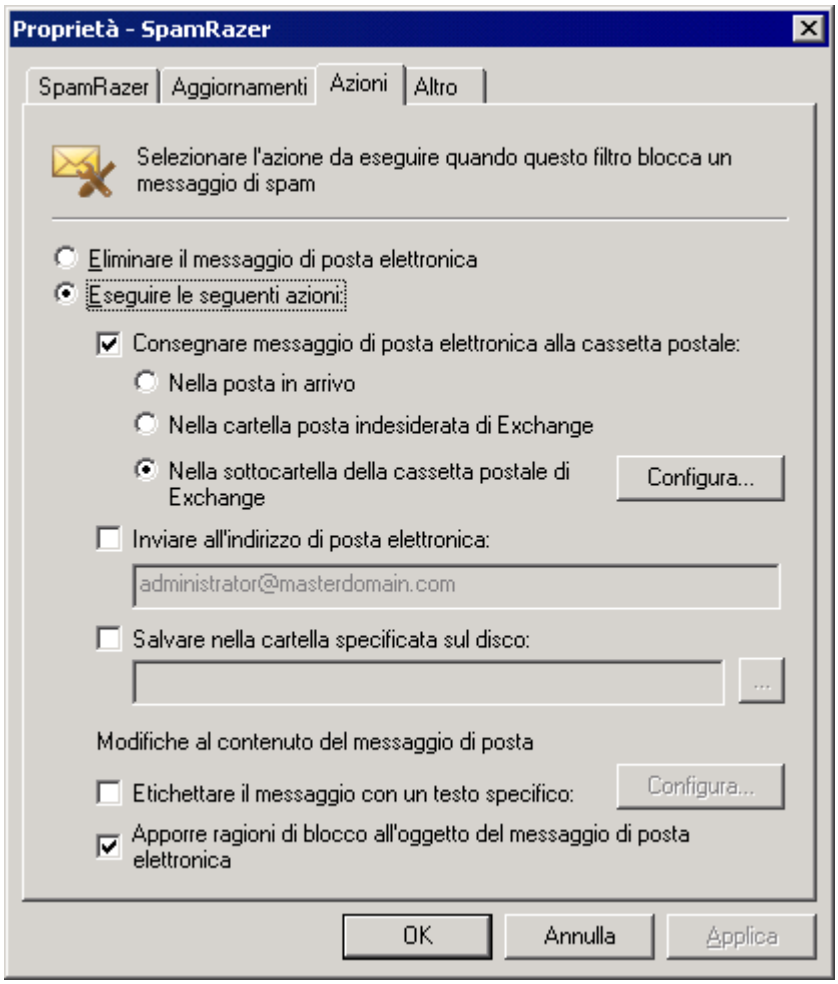
Le schede **Azioni** e **Altro** nelle finestre di dialogo del filtro antispam

definiscono le operazioni da eseguire sui messaggi di posta elettronica contrassegnati come spam. È possibile configurare azioni diverse per ciascuno dei filtri antispam disponibili. Questa caratteristica consente, in modo opportuno, di separare le cartelle ai fini dell'archiviazione della posta spam individuata da ogni filtro. In questo modo, è possibile identificare immediatamente il motivo per cui il messaggio di posta elettronica è stato contrassegnato come spam ed è più facile eseguire operazioni su messaggi di posta bloccati da un determinato filtro.

- **Esempio:** si potrebbe voler eliminare i messaggi di posta elettronica identificati dal filtro antispam della black list, ma agire diversamente nei confronti dei messaggi di spam identificati dal filtro del controllo parola chiave.

NOTA: le opzioni presenti nella scheda delle azioni sono identiche per tutti i filtri antispam, eccetto per la white list (filtri antispam evitati) e Nuovi mittenti (impossibile spostare lo spam nella cartella Posta indesiderata).

Configurazione delle azioni antispam



Schermata 54 - Configurazione dell'azione da intraprendere

1. Nella scheda **Azioni**, selezionare un'opzione che definisca quale azione intraprendere sui messaggi di posta elettronica contrassegnati come spam:

- **Elimina il messaggio di posta elettronica** - elimina un messaggio di posta elettronica bloccato dal filtro antispam in questione. Le altre azioni antispam sono disabilitate con l'eliminazione del messaggio di posta elettronica.
- **Consegna il messaggio di posta elettronica nella cassetta postale** - scegliere la cartella dove consegnare il messaggio di posta elettronica:
  - **Nella posta in arrivo** - Usare questa opzione per indirizzare lo spam nella posta in arrivo dell'utente.
  - **Nella cartella di posta indesiderata di Exchange** - Usare questa opzione per indirizzare tutto lo spam verso la cartella predefinita destinata ai messaggi indesiderati dell'utente.
  - **Nella sottocartella della cassetta postale di Exchange** - Usare questa opzione per indirizzare tutto lo spam verso una cartella specifica nella cassetta postale dell'utente. Fare clic su Configura per avviare la finestra di dialogo Sposta nella cartella Exchange e digitare la cartella nella quale spostare il messaggio di spam.
    - **Esempio 1:** Digitare **Presunto spam** per creare una cartella personalizzata sullo stesso livello della cartella di posta in arrivo.
    - **Esempio 2:** Digitare **Posta in arrivo\Presunto spam** per creare una cartella personalizzata all'interno della cartella di posta in arrivo.

    NOTA 1: questa opzione richiede che:
    - GFI MailEssentials sia installato sul computer Microsoft Exchange Server. Se GFI MailEssentials non è installato sul Microsoft Exchange Server consultare il capitolo Spostamento dei messaggi di spam nelle cartelle della cassetta postale dell'utente a pagina 122 di questo manuale.
    - La modalità Active Directory sia abilitata
    - Sia presente Microsoft Exchange Server 2000/2003 o Microsoft Exchange Server 2007 con Mailbox Server Role

    NOTA 2: per Microsoft Exchange 2010 è richiesto un utente dedicato per abilitare questa opzione. Nella finestra di dialogo Azioni fare clic su **Configura** e fare clic su **Specifica account utente** per specificare l'utente dedicato. Nella finestra di configurazione Sposta nella cartella di Exchange, selezionare una delle seguenti opzioni:
    - **Spostare lo spam utilizzando un utente creato automaticamente** - Selezionare questa opzione per permettere a GFI MailEssentials di creare automaticamente un utente in possesso di tutti i diritti richiesti.
    - **Spostare lo spam utilizzando il seguente account utente** - Selezionare questa opzione per utilizzare un utente creato manualmente. Specificare le credenziali (dominio\nome utente e password) di un utente dedicato e fare clic su **Imposta diritti di accesso** per assegnare i diritti richiesti all'utente specificato.

NOTA: le credenziali utente specificate manualmente devono essere dedicate solamente a questa funzione. Il nome utente, password o altre proprietà NON devono essere cambiate da Microsoft Exchange o Active Directory, in caso contrario la funzionalità Sposta nella cartella Exchange non funzionerà.

- **Invia il messaggio all'indirizzo di posta elettronica** - invia all'indirizzo di posta elettronica indicato il messaggio etichettato come spam.
  - **Esempio:** un indirizzo di posta elettronica di una cartella pubblica. In questo modo, a un soggetto può essere assegnato il compito di controllare periodicamente i messaggi di posta elettronica contrassegnati come spam e identificare quelli che potrebbero essere stati contrassegnati come spam per errore. Questa funzionalità è inoltre utilizzabile per manualmente migliorare ulteriormente le regole antispam.

  L'oggetto del messaggio di posta è nel formato
- **Salva nella cartella specificata sul disco** - salva il messaggio di posta elettronica individuato come spam nel percorso specificato.
  - **Esempio:** "C:\Spam\".

  Il nome del file del messaggio di posta elettronica salvato ha il seguente formato:

  `[Sender_recipient_subject_number_.eml]` (per esempio: `C:\Spam\jim@comp.com_bob@comp.com_MailOffers_1_.eml`)
- **Etichetta il messaggio con un testo specifico** - selezionare questa opzione per aggiungere un'etichetta all'oggetto del messaggio di posta elettronica. Fare clic su **Configura** per modificare le opzioni di etichettatura. Nella finestra di dialogo Etichetta messaggio di posta elettronica, inserire il testo da usare per l'etichettatura e specificare la posizione dell'etichetta:
  - **Anteponi all'oggetto** - per inserire l'etichetta specificata all'inizio (ossia come prefisso) dell'oggetto del messaggio.
    - **Esempio:** "[SPAM]Posta Web gratuita".
  - **Posponi all'oggetto** - per inserire l'etichetta specificata alla fine (ossia come suffisso) dell'oggetto del messaggio.
    - **Esempio:** "Posta Web gratuita[SPAM]".
  - **Aggiungi etichetta in un'intestazione X…** - per aggiungere l'etichetta specificata come nuova intestazione X del messaggio di posta elettronica. In questo caso, l'Intestazione X deve avere il seguente formato:

    `X-GFIME-SPAM: [TESTO ETICHETTA]`

    `X-GFIME-SPAM-MOTIVO: [MOTIVO]`

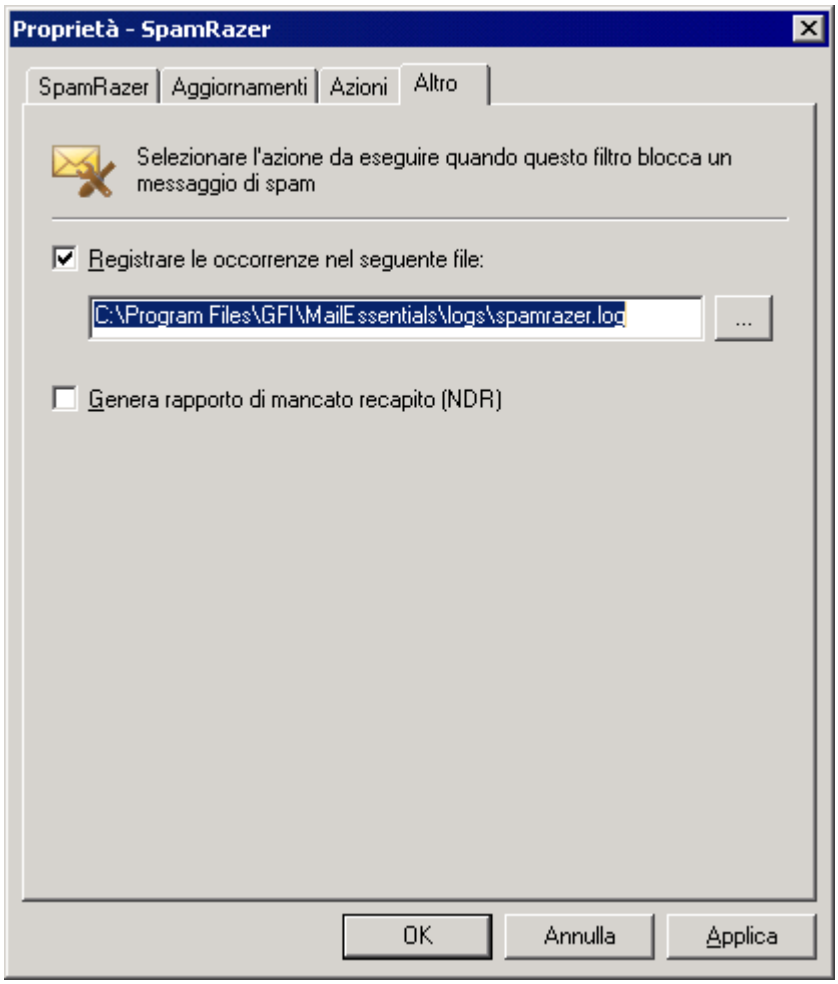
    - **Esempio:**

    `X-GFIME-SPAM: [Questo è uno SPAM]`

    `X-GFIME-SPAM-MOTIVO: [DNSBL Verifica non riuscita - Inviato da dominio nella Black list]`

- **Apponi il motivo del blocco all'oggetto del messaggio di posta elettronica** - Abilitando questa opzione il nome del filtro che ha bloccato il messaggio e il motivo del blocco vengono apposti all'oggetto del messaggio bloccato.

Altre opzioni



Schermata 55 - La scheda Altre azioni

Selezionare la scheda **Altro** per specificare una serie di azioni facoltative:

- **Registrare le attività nel seguente file** - consente di registrare l'attività del messaggio di spam in un file di registro a scelta.
- **Generare rapporto di mancato recapito (NDR)** - crea e invia un falso NDR. In questo modo si determina la rimozione del proprio indirizzo di posta elettronica dal data base della maggioranza dei software di bulk mailing (mailing di massa). Inoltre, è possibile avvalersi di questa caratteristica per informare il mittente che il suo messaggio di posta elettronica è stato considerato come spam.

NOTA: per personalizzare il falso NDR, modificare "ndr.xml" situato nella directory MailEssentials\templates usando notepad o qualsiasi editor di formato XML.

4.2.15 Azioni antispam generali

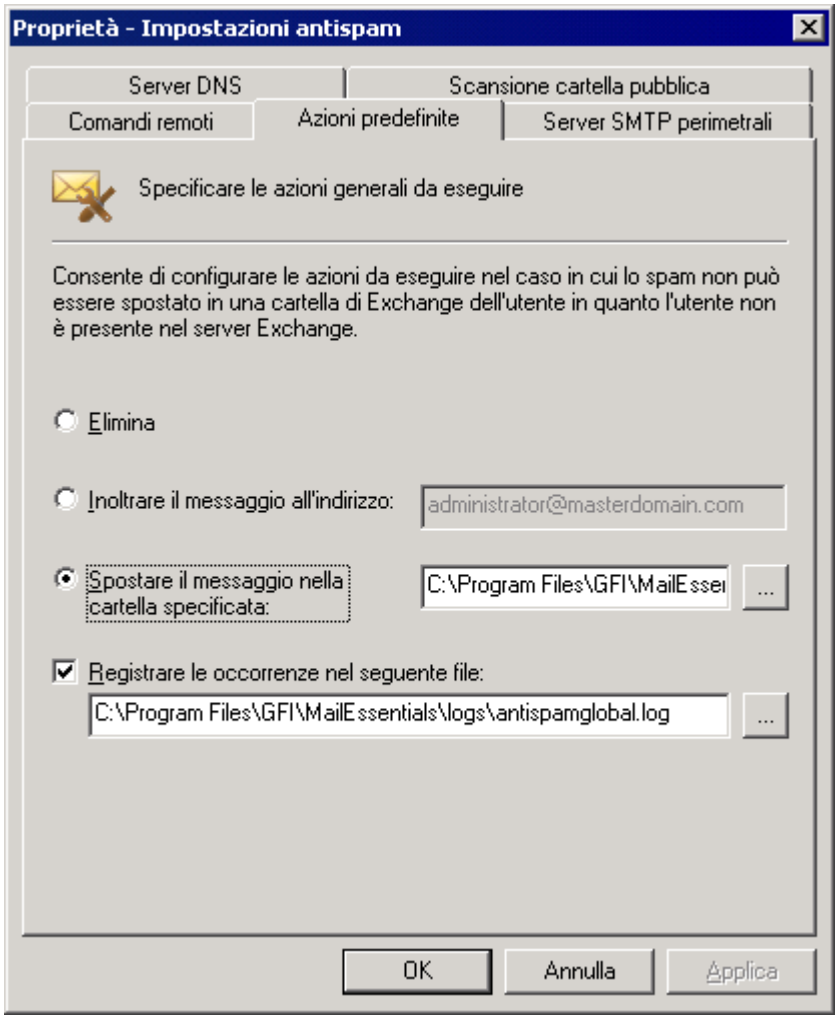
Una gran quantità di spam è inviata a indirizzi di posta elettronica che

non esistono più sul proprio server. In genere, questi messaggi vengono semplicemente eliminati. Tuttavia, per risolvere problemi o a fini di valutazione si potrebbe volere spostare questi messaggi di posta elettronica in una cartella oppure inoltrarli a un particolare indirizzo di posta elettronica.

NOTA: questa sezione si applica soltanto alle installazioni su Microsoft Exchange Server 2000/2003/2007 e che utilizzano la funzione **Inoltra nella cartella di spam dell'utente**. Su altri server, la scheda Azioni antispam generali non comparirà.

Configurazione delle Azioni antispam generali

1. Fare clic con il pulsante destro del mouse sul nodo **Antispam ► Impostazioni antispam** e selezionare **Proprietà**.



Schermata 56 - Azioni generali

2. Selezionare la scheda **Azioni generali** e scegliere se:

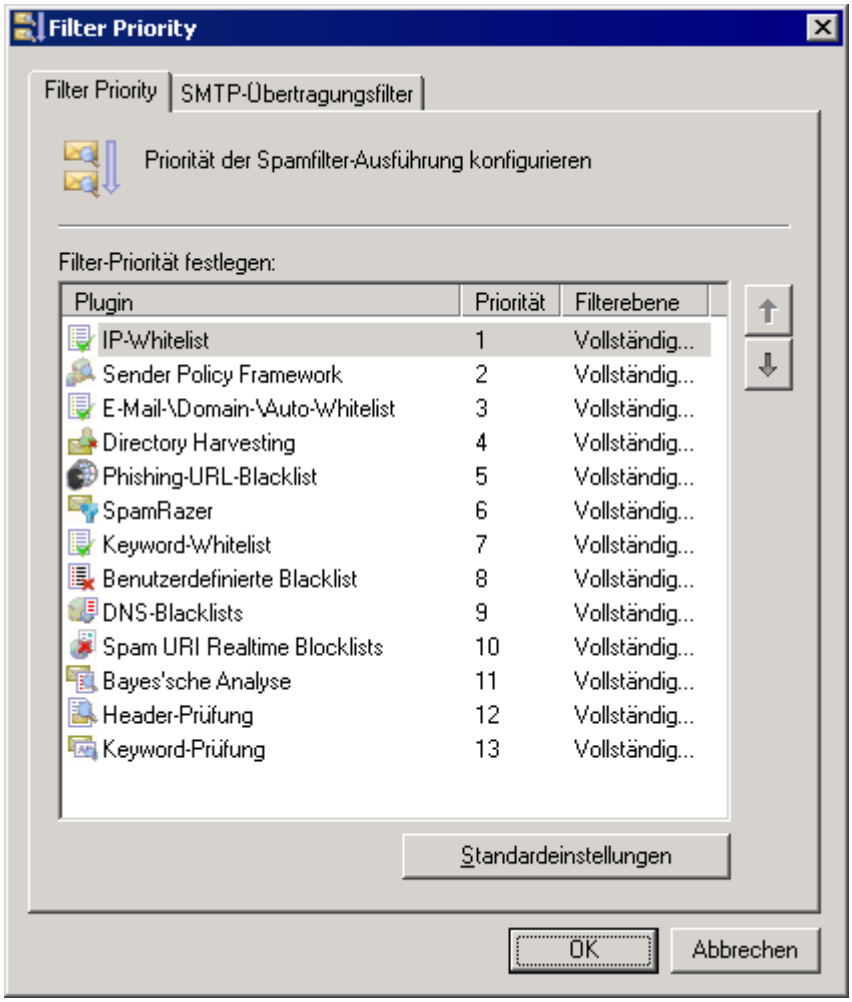
- eliminare il messaggio di posta elettronica
- inoltrarlo verso un indirizzo di posta elettronica
- spostarlo verso una cartella specificata.

3. Selezionare **Registrare le attività nel seguente file** per registrare lo spam in un file di registro.

4.2.16 Ordinare i filtri antispam in base a priorità

In GFI MailEssentials è possibile personalizzare l'ordine con cui i controlli antispam devono essere applicati ai messaggi in arrivo.

NOTA: è possibile stabilire l'ordine di priorità di tutti i filtri disponibili tranne quello del filtro Nuovi mittenti, che è sempre automaticamente impostato sulla priorità più bassa. Ciò è dovuto al fatto che il filtro dipende dai risultati dei controlli della white list e degli altri filtri antispam.



Schermata 57 - Attribuzione delle priorità ai filtri

1. Fare clic con il pulsante destro del mouse sul nodo **Antispam ► Priorità filtro** e selezionare **Proprietà**.

2. Selezionare il filtro desiderato e fare clic sul pulsante (su) per attribuire una priorità più alta al filtro selezionato oppure fare clic sul pulsante (giù) per attribuire una priorità inferiore al filtro selezionato.

NOTA: facendo clic sul pulsante **Impostazioni predefinite** si ripristineranno le priorità dei filtri nell'ordine predefinito.

3. Fare clic sul pulsante **OK** per completare la configurazione. Le modifiche avranno effetto immediato.

4.3 Declinazioni di responsabilità

Le declinazioni di responsabilità sono un testo standard aggiunto in fondo o all'inizio di ciascun messaggio di posta elettronica in uscita utilizzate per ragioni legali e/o di marketing. Queste proteggono le aziende da potenziali minacce legali derivanti dal contenuto di un messaggio di posta elettronica e aggiungono informazioni descrittive riguardo ai prodotti/servizi offerti.

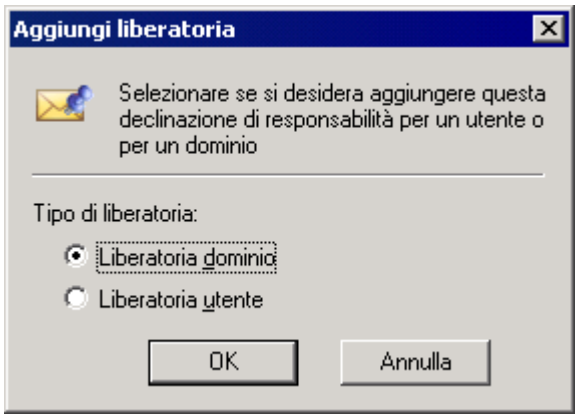
Note importanti

1. Le declinazioni di responsabilità sono aggiunte solo ai messaggi di posta elettronica in uscita.

2. Affinché le modifiche abbiano effetto immediato, riavviare i servizi IIS e GFI MailEssentials dopo aver disabilitato una declinazione di responsabilità.

4.3.1 Configurazione delle declinazioni di responsabilità

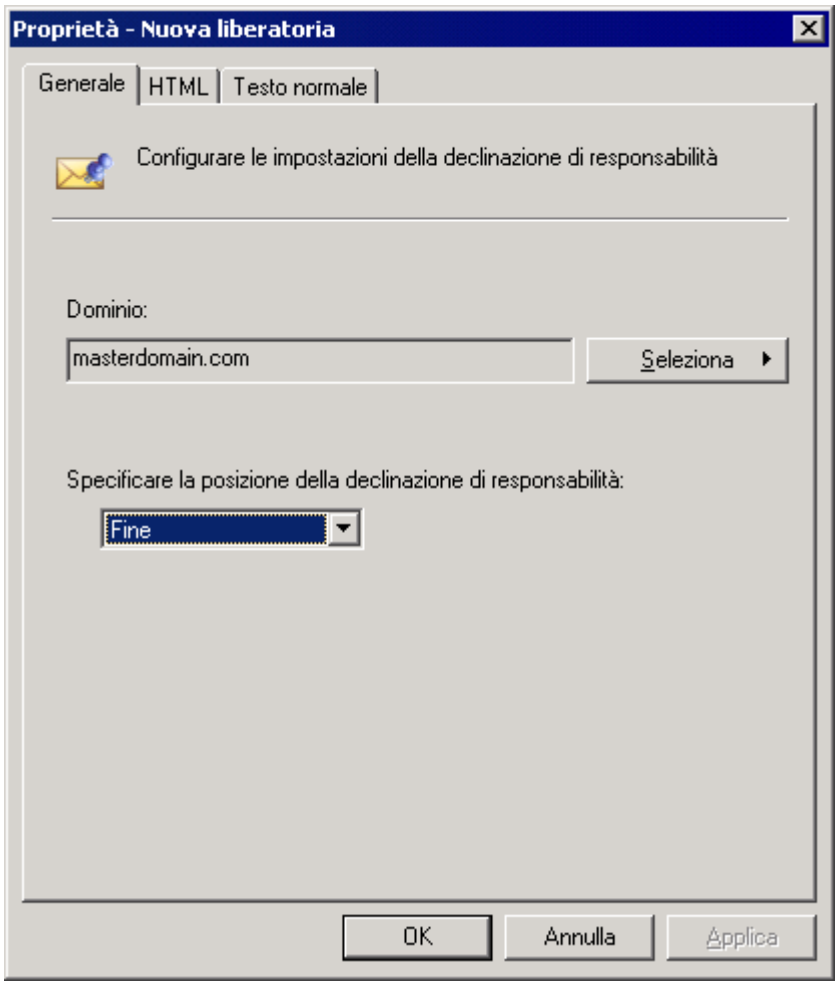
1. Fare clic con il pulsante destro del mouse sul nodo **Gestione posta elettronica ► Declinazioni di responsabilità** e selezionare **Nuovo ► Declinazione di responsabilità.**



Schermata 58 - Selezione della declinazione di responsabilità per un utente o un dominio

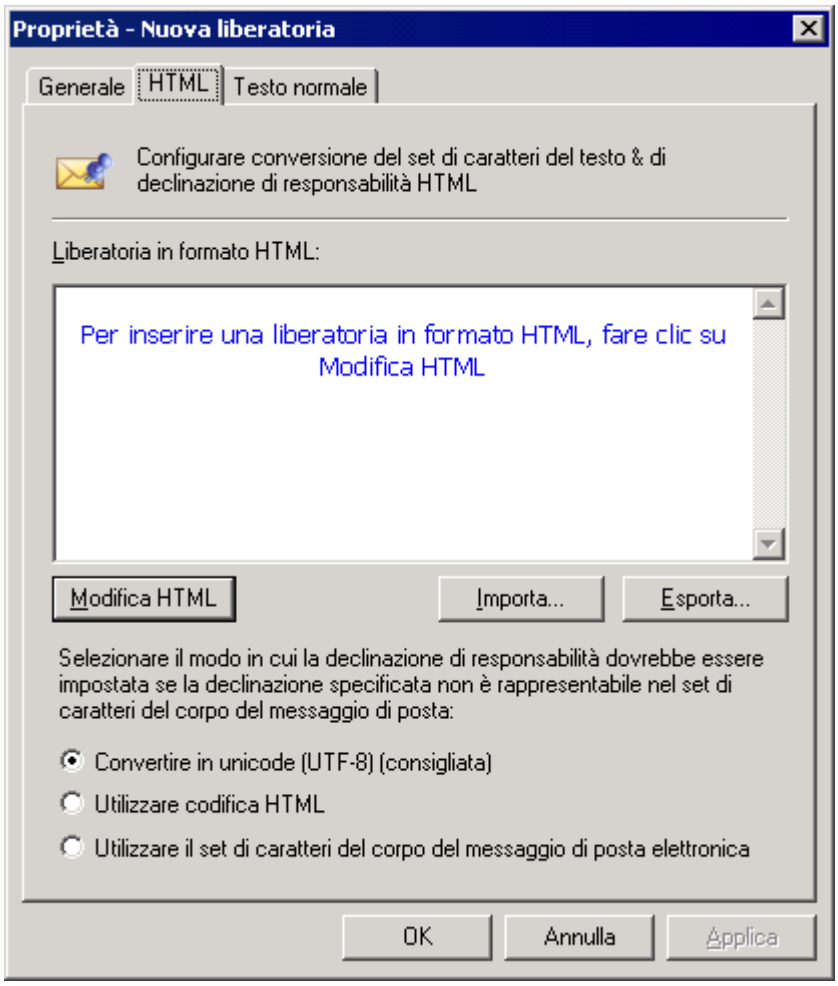
2. Selezionare:

- **Dominio** - Scegliere il dominio dall'elenco di domini configurati. Tutti i messaggi di posta elettronica inviati da quel dominio conterranno la declinazione di responsabilità.
- **Utente** - Specificare un utente o un gruppo di utenti a cui aggiungere l'esclusione di responsabilità per i messaggi di posta elettronica in uscita. Se GFI MailEssentials è installato in modalità Active Directory, è possibile selezionare gli utenti o gruppi di utenti direttamente da Active Directory. Diversamente, va indicato l'indirizzo di posta elettronica SMTP dell'utente.



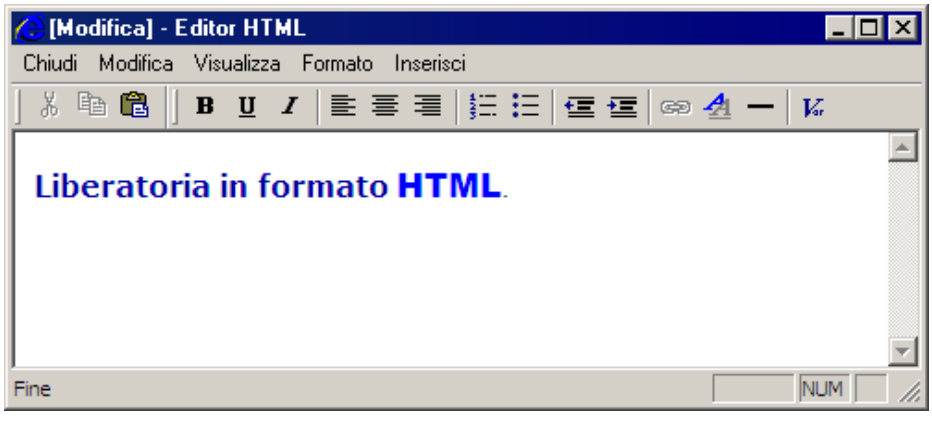
Schermata 61- Proprietà generali nuova declinazione di responsabilità

3. Nella scheda **Generale** fare clic su **Seleziona** per cambiare dominio o utente. Selezionare l'opzione **All'inizio** o **In fondo** se si vuole inserire la declinazione di responsabilità all'inizio o in fondo al messaggio di posta elettronica.



Schermata 62 - Declinazione di responsabilità HTML

4. Per aggiungere una declinazione di responsabilità in HTML, selezionare la scheda HTML. Fare clic su **Modifica HTML** per eseguire l'editor HTML della declinazione di responsabilità e modificare il testo della declinazione di responsabilità HTML.



Schermata 63 - L'editor HTML della declinazione di responsabilità

NOTA 1: per le declinazioni di responsabilità in HTML, usare l'editor come una semplice applicazione di elaborazione testi. È possibile inserire variabili nel testo della declinazione di responsabilità tramite l'opzione del menu **Inserisci**. Le variabili sono campi il cui contenuto, nel messaggio di posta elettronica, è sostituito dal nome del vero

destinatario o mittente. Nel testo di una declinazione di responsabilità inserire i seguenti campi:

- [Data]
- [Nome del mittente]
- [Indirizzo di posta elettronica del mittente]
- [Nome del destinatario]
- [Indirizzo di posta elettronica del destinatario]

NOTA 2: le variabili “nome del destinatario visualizzato” e “indirizzo di posta elettronica del destinatario” vengono sostituite soltanto se il messaggio di posta elettronica è inviato a un unico destinatario. Se i messaggi di posta elettronica vengono inviati a più destinatari, le variabili sono sostituite da “destinatari”.

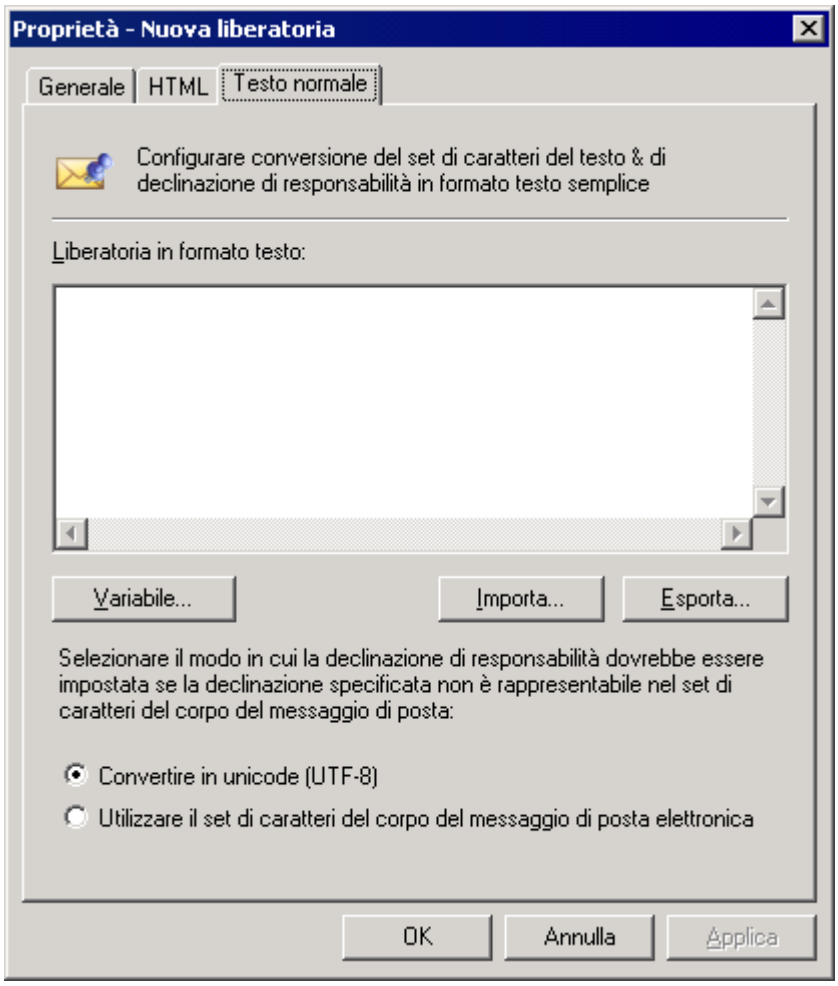
5. Fare clic su **Chiudi** per aggiungere la declinazione di responsabilità HTML.

6. Specificare la codifica da utilizzare per la declinazione di responsabilità HTML se il set di caratteri del corpo del messaggio di posta non è HTML:

- **Utilizzare codifica HTML** - utilizzare la codifica HTML per definire set di caratteri per il corpo del messaggio e per la declinazione di responsabilità. Quest’opzione è consigliata.
- **Converti a Unicode** - converte sia il corpo del messaggio di posta elettronica che le declinazioni di responsabilità a Unicode così che entrambi vengano correttamente visualizzati.
- **Utilizza set di caratteri del corpo del messaggio** - la declinazione di responsabilità viene convertita nel set di caratteri del corpo del messaggio di posta elettronica.

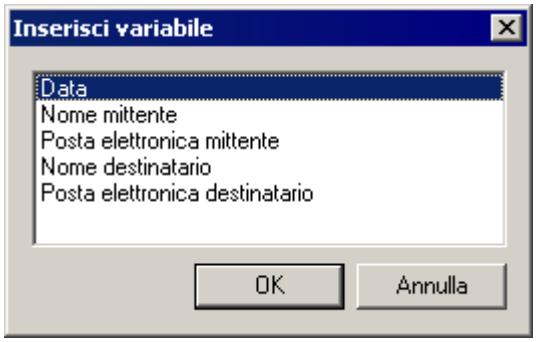
  Nota: se è selezionata questa opzione, parte del testo di declinazione di responsabilità potrebbe non essere visualizzata correttamente.

7. Importare o esportare una declinazione di responsabilità in HTML in formato .htm o .html utilizzando i pulsanti **Importa** ed **Esporta**.



Schermata 64 - Declinazione di responsabilità in testo semplice

8. È possibile includere una versione della declinazione di responsabilità basata su testo, per il solo uso in messaggi di posta elettronica di testo normale. Selezionare **Testo semplice** e inserire il testo direttamente nel campo **Declinazione di responsabilità in formato testo**. Usare il pulsante **Variabile…** per aggiungere le variabili.



Schermata 65 - Inclusione di variabili nella declinazione di responsabilità

NOTA: le variabili “nome del destinatario visualizzato” e “indirizzo di posta elettronica del destinatario” vengono sostituite soltanto se il messaggio di posta elettronica è inviato a un unico destinatario. Se i messaggi di posta elettronica vengono inviati a più destinatari, le variabili sono sostituite da “destinatari”.

9. Specificare la codifica da utilizzare per la declinazione di responsabilità in formato testo semplice se il set di caratteri del corpo del messaggio di posta non è testo semplice:

- **Converti a Unicode** - converte sia il corpo del messaggio di posta elettronica che le declinazioni di responsabilità a Unicode così che entrambi vengano correttamente visualizzati.
- **Utilizza set di caratteri del corpo del messaggio** - la declinazione di responsabilità viene convertita nel set di caratteri del corpo del messaggio di posta elettronica.

  Nota: se è selezionata questa opzione, parte del testo di declinazione di responsabilità potrebbe non essere visualizzata correttamente.

10. Importare o esportare una declinazione di responsabilità in formato testo semplice utilizzando i pulsanti **Importa** ed **Esporta**.

La nuova declinazione di responsabilità viene visualizzata nel pannello di destra della console di GFI MailEssentials configuration. Per attribuire alla nuova declinazione di responsabilità un nome più utile, fare clic con il tasto destro sulla declinazione di responsabilità e selezionare **Rinomina**.

4.3.2 Abilitazione e disabilitazione delle declinazioni di responsabilità

Per impostazione predefinita, le nuove declinazioni di responsabilità vengono abilitate automaticamente. Per abilitare o disabilitare una declinazione di responsabilità:

1. Fare clic con il pulsante destro del mouse per disabilitare la declinazione di responsabilità.

2. Selezionare **Disabilita** o **Abilita** per eseguire l'operazione desiderata.

4.4 Risposte automatiche

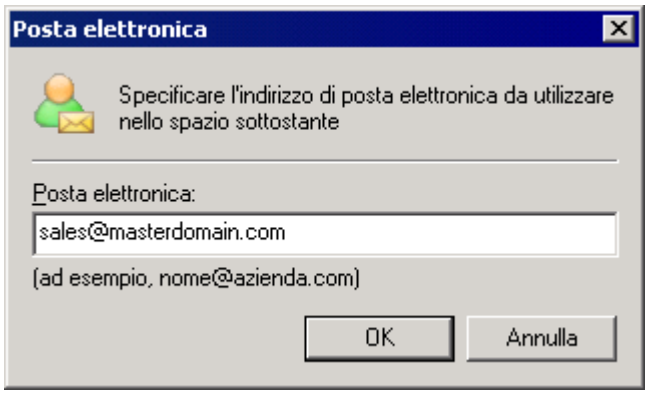
La caratteristica della risposta automatica (*Auto reply*) consente di inviare risposte automatizzate a determinati messaggi di posta elettronica in arrivo. Si può indicare una risposta automatica diversa per ciascun indirizzo od oggetto di un messaggio di posta elettronica. Per personalizzare un messaggio di posta elettronica, è possibile utilizzare variabili in una risposta automatica.

Note importanti

1. Assicurarsi che ciascuna riga non contenga più di 30-40 caratteri oppure non comprenda gli "a capo". Questo perché alcuni server di posta meno recenti troncano la riga a 30-40 caratteri.

4.4.1 Configurazione delle risposte automatiche

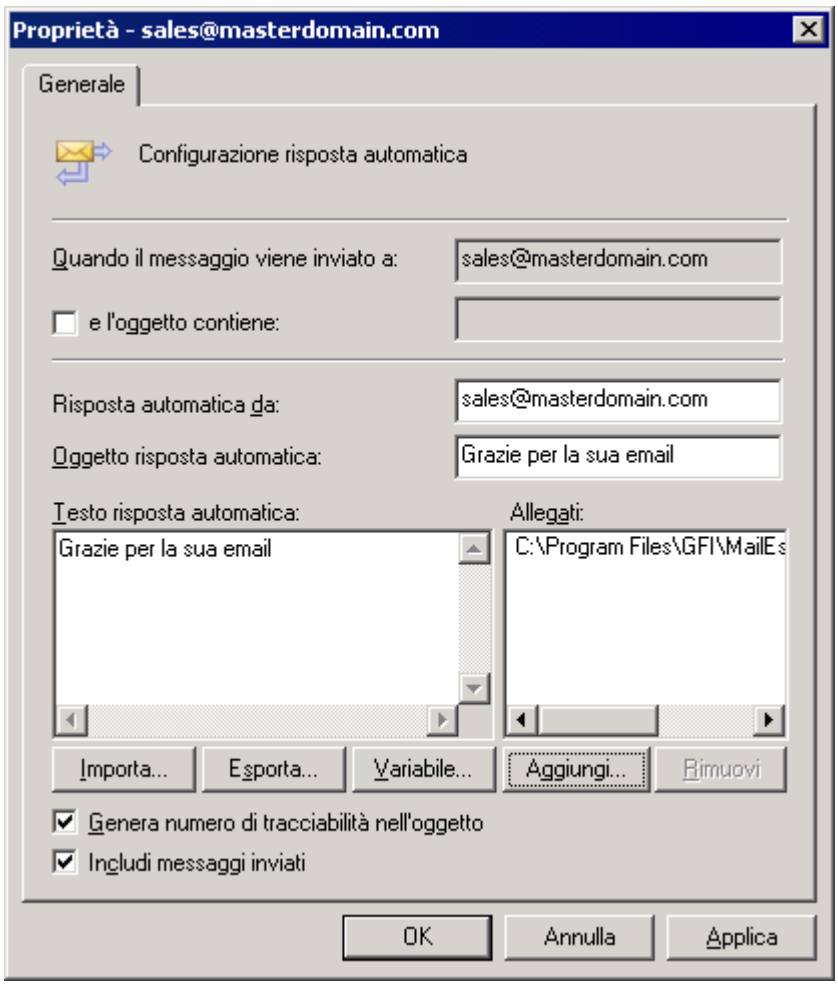
1. Fare clic con il pulsante destro del mouse sul nodo **Gestione posta elettronica ► Risposte automatiche** e selezionare **Nuovo ► Risposta automatica.**



Schermata 62 - Creazione di una nuova risposta automatica

2. Inserire l'indirizzo di posta elettronica per configurare una risposta automatica e fare clic su **OK**.

- **Esempio** - se si specifica sales@master-domain.com, il mittente di un messaggio di posta elettronica in arrivo inviato a questo indirizzo di posta elettronica riceverà una risposta automatica.



Schermata 63 - Proprietà della risposta automatica

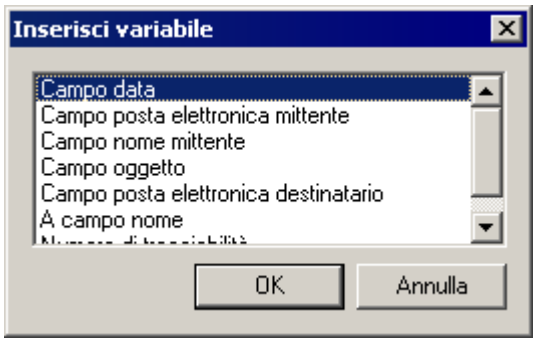
3. Selezionare la casella di controllo **e l'oggetto contiene** per abilitare le risposte automatiche a messaggi di posta elettronica contenenti un testo specifico nel campo dell'oggetto.

4. Nel campo **Risposta automatica da:** specificare un indirizzo di posta elettronica se è necessaria una risposta automatica da un indirizzo di posta elettronica diverso da quello a cui è stato inviato il messaggio in arrivo.

5. L'oggetto della risposta automatica può invece essere indicato nel campo **Oggetto risposta automatica**.

6. È possibile specificare il testo da visualizzare nel messaggio di risposta automatica nella casella di modifica **Testo risposta automatica**.

NOTA: è possibile importare il testo della risposta automatica da un file di testo mediante il pulsante **Importa…**



Schermata 64 - Finestra di dialogo delle variabili

7. Fare clic su **Variabile…** per personalizzare le risposte automatiche mediante le variabili. Selezionare il campo della variabile che si desidera inserire e fare clic su **OK**. Le variabili disponibili sono:

- **Campo data** - per inserire la data di invio del messaggio di posta elettronica.
- **Campo messaggio di posta elettronica da** - per inserire l'indirizzo di posta elettronica del mittente.
- **Campo nome da** - per inserire il nome del mittente visualizzato.
- **Campo oggetto** - per inserire l'oggetto del messaggio di posta elettronica.
- **Campo messaggio di posta elettronica a** - per inserire l'indirizzo di posta elettronica del destinatario.
- **Campo nome a** - per inserire il nome visualizzato del destinatario.
- **Numero di tracciabilità** - per inserire il numero di tracciabilità, ove generato.

8. Fare clic su **Aggiungi…** e selezionare eventuali allegati da inviare con il messaggio di risposta automatica. Rimuovere gli allegati usando il pulsante **Rimuovi**.

9. Se si desidera includere il messaggio di posta elettronica in arrivo nella risposta automatica, selezionare l'opzione **Includi messaggio di posta elettronica inviato**.

10. Selezionare l'opzione **Genera numero di tracciabilità nell'oggetto** per generare un numero di tracciabilità nelle risposte automatiche.

NOTA: questa funzionalità consente, per esempio, ai clienti di rispondere riportando un numero di tracciabilità di modo che il personale sia in grado di tracciare i messaggi di posta elettronica in

modo più uniforme.

11. Fare clic sul pulsante **OK** per completare le impostazioni.

Per impostazione predefinita, i numeri di tracciabilità sono generati utilizzando il seguente formato:

- ME_AAMMGG_nnnnnn

Dove:

- **ME -** etichetta di GFI MailEssentials.
- **AAMMGG -** formato data in anno, mese e giorno.
- **nnnnnn -** numero di tracciabilità generato automaticamente.

4.5 Server di elenco

I server di elenco consentono di creare due tipi di liste di distribuzione:

1. Una lista d'iscrizione a newsletter - utilizzato per creare liste di iscrizione per la newsletter di un'azienda o di un prodotto alla quale gli utenti possono iscriversi o annullare l'iscrizione.

2. Una lista di discussione - consente a un gruppo di persone di sostenere discussioni tramite la posta elettronica, poiché ogni membro della lista riceve il messaggio di posta elettronica inviato alla lista da un altro utente.

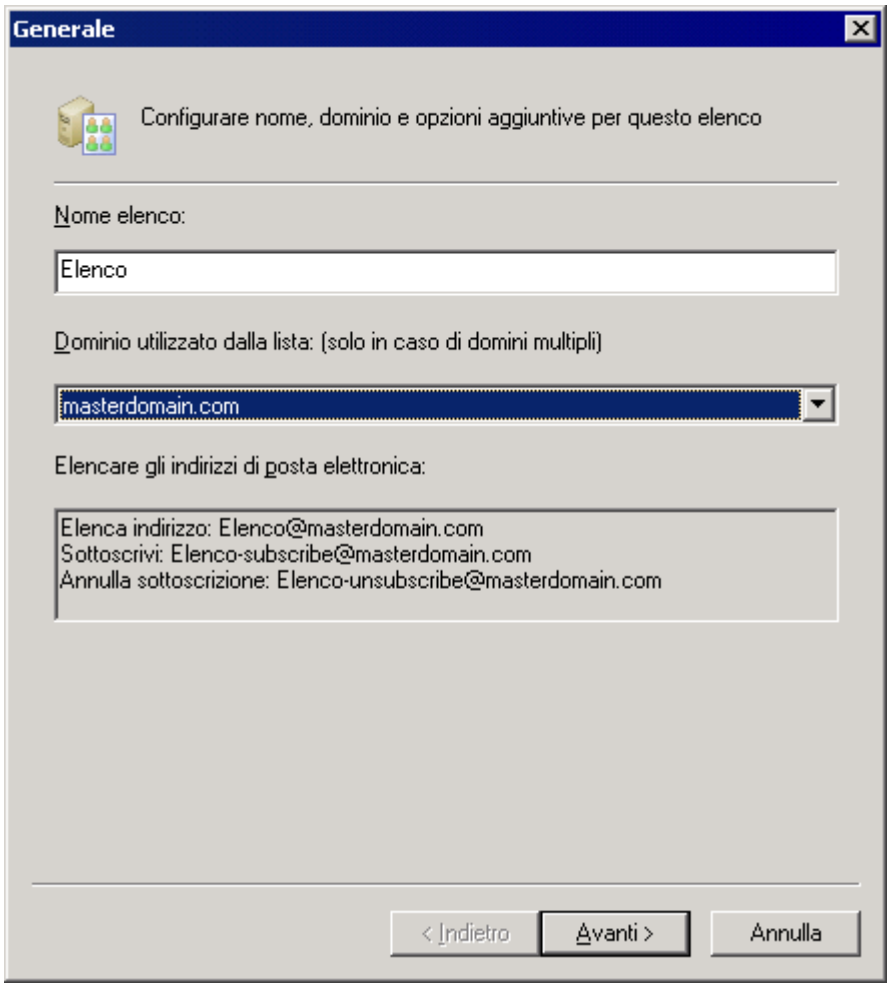
Prerequisiti

1. Verificare se è installato MSMQ. In caso contrario, procedere alla sua installazione. Consultare la "Guida introduttiva" di GFI MailEssentials:

http://www.gfi-italia.com/it/me/mes14gsgmanual_it.pdf

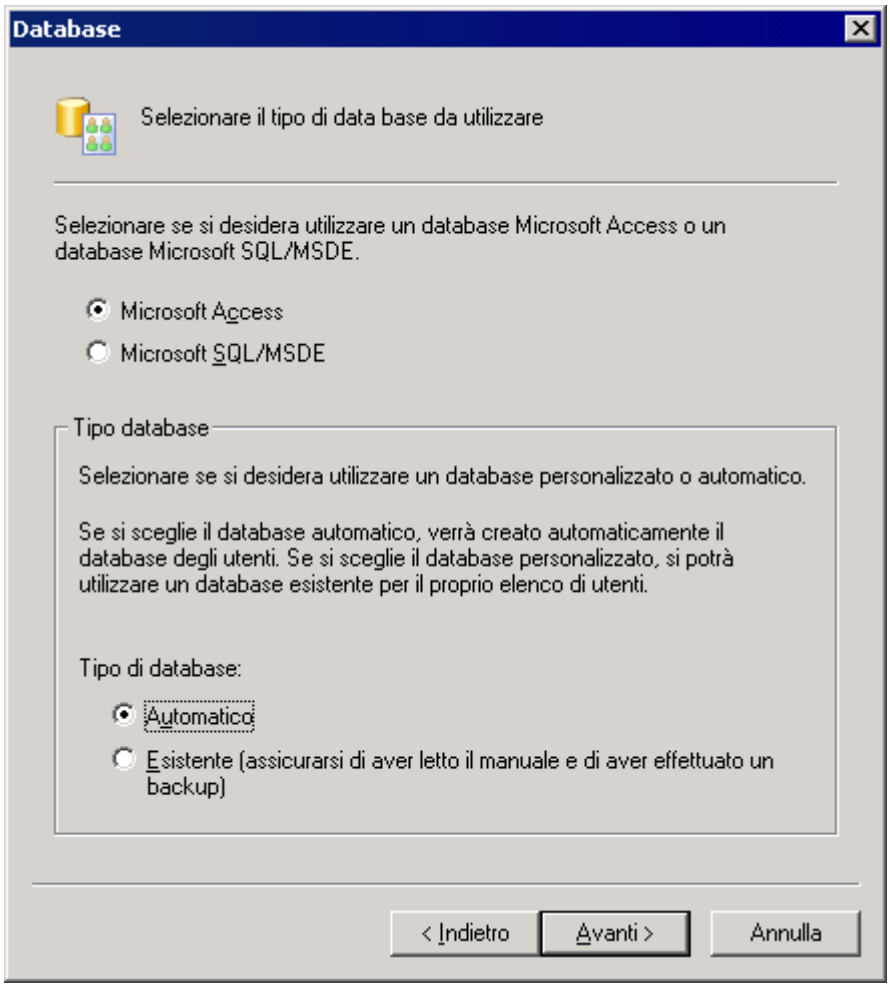
4.5.1 Creazione di una newsletter o di una lista di discussione

1. Dalla console di GFI MailEssentials configuration fare clic con il pulsante destro del mouse su **Gestione posta elettronica ► Elenco Server** e selezionare **Nuovo ► Newsletter** o **Elenco discussione**.



Schermata 65 - Creazione di una lista di iscrizione a newsletter

2. Nel campo **Nome elenco:** inserire un nome di una nuova lista e selezionare un dominio per la lista (in caso di più domini). Fare clic su **Avanti** per continuare la configurazione.



Schermata 66 - Specificazione del back-end del data base

3. Selezionare **Microsoft Access** o **Microsoft SQL Server/MSDE** come data base e dal gruppo **Tipo di data base** scegliere se GFI MailEssentials deve creare un nuovo data base o connettersi a un data base esistente. Fare clic su **Avanti** per continuare.

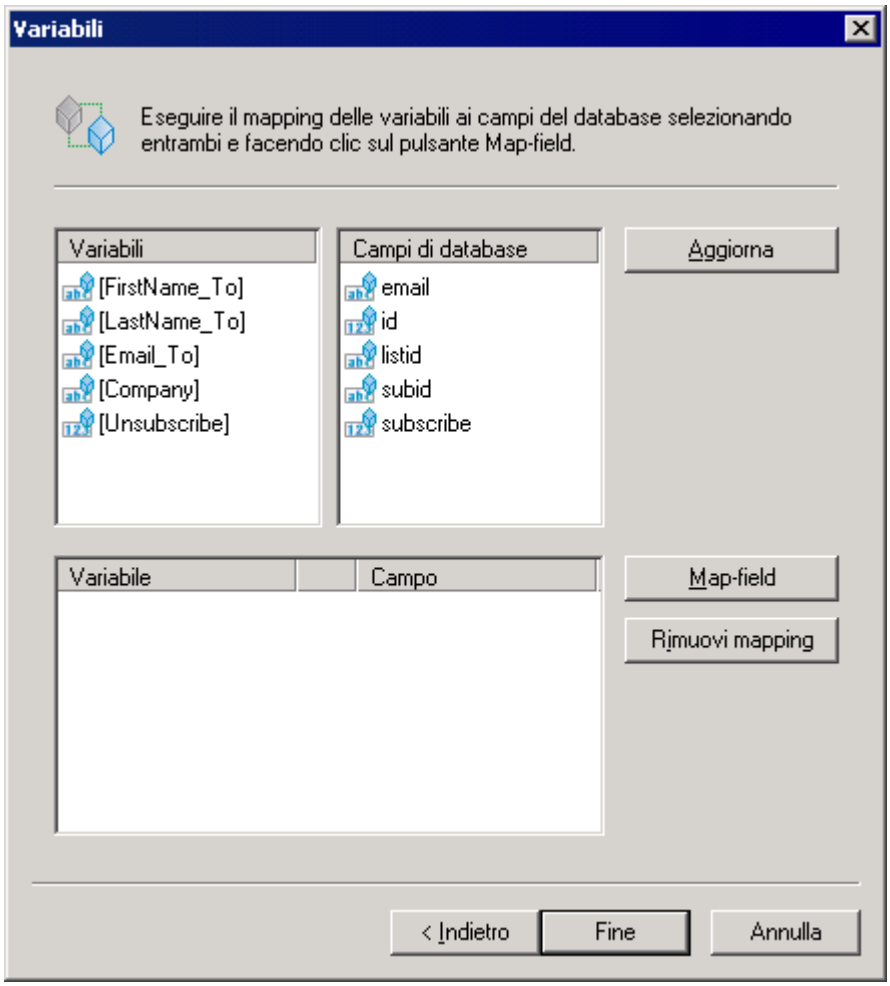
NOTA 1: per piccole liste, cioè fino a 5.000 membri, è possibile utilizzare come terminale Microsoft Access.

NOTA 2: per creare un nuovo data base, selezionare l'opzione **Automatico**.

4. Configurare il tipo di data base selezionato per archiviare la newsletter/lista di iscritti alla discussione. Le opzioni disponibili sono:

Tipo di database	Impostazioni del database
Microsoft Access con opzione Automatico	Indicare la posizione in cui si desidera creare il nuovo data base nella casella di modifica File
Microsoft Access con opzione Esistente	Nel campo de File, specificare il percorso al data base Microsoft Access esistente contenente gli iscritti alla newsletter/discussione. Dall'elenco a discesa Tabella, selezionare la tabella in cui è archiviato l'elenco degli iscritti.
Microsoft SQL Server con opzione Automatico	È necessario configurare il nome del server SQL, le credenziali di accesso e il data base da utilizzare per memorizzare l'elenco di iscritti alla newsletter/discussione.
Microsoft SQL con opzione Esistente	È necessario specificare il nome del server SQL e le credenziali di accesso e selezionare poi il data base e la tabella contenenti l'elenco degli iscritti.

5. Se si è selezionato qualsiasi tipo di data base con l'opzione **Automatico,** fare clic sul pulsante **Fine** per terminare la procedura guidata oppure fare clic su **Avanti** per continuare la configurazione.



Schermata 67 - Mapping dei campi personalizzati

6. Per eseguire il mapping tra i campi richiesti e i campi personalizzati

del data base, è necessario selezionare una variabile dall'elenco delle **Variabili** e l'opzione corrispondente **Campo database,** quindi fare clic sul pulsante **Mappa campo**. Fare clic su **Fine** per completare la configurazione. I campi per cui eseguire il mapping sono:

- **[Inviare un messaggio di posta elettronica_A]** - Valorizza il mapping al campo di una stringa contenente l'indirizzo di posta elettronica di un iscritto.
- **[Annulla l'iscrizione]** - Esegue il mapping al campo di un valore intero (o Booleano) usato per stabilire se l'utente è iscritto o meno alla lista.
- **[NomeProprio_A]** - Eseguire il mapping al campo di una stringa contenente il nome proprio di un iscritto.
- **[Cognome_A]** - Eseguire il mapping al campo di una stringa contenente il cognome di un iscritto.
- **[Azienda]** - Eseguire il mapping al campo di una stringa contenente il nome dell'azienda di un iscritto.

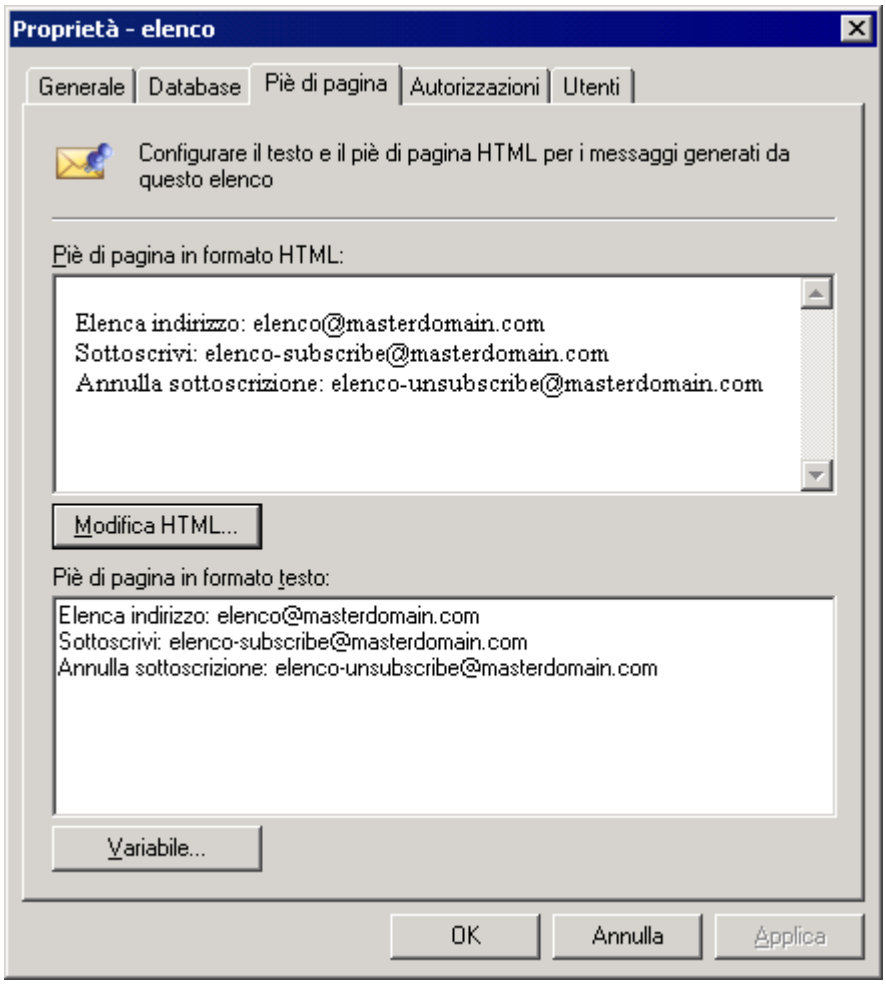
4.5.2 Configurazione delle proprietà avanzate della newsletter/lista di discussione

Dopo aver creato una nuova lista, è possibile configurare altre opzioni che consentono di personalizzare gli elementi e il comportamento della lista. Le opzioni disponibili sono:

- Creazione di un piè di pagina personalizzato - permette di configurare un piè di pagina personalizzato in formato HTML o in formato testo. Tale piè di pagina verrà aggiunto a ogni messaggio di posta elettronica.
- Impostazione delle autorizzazioni dell'elenco - consente di specificare chi può inviare un messaggio di posta elettronica all'elenco. Se non si protegge la lista, chiunque sarà in grado di inviare un messaggio di posta elettronica all'intera lista mandando un messaggio all'indirizzo generale della lista.

  NOTA: le autorizzazioni non sono configurabili per le liste di discussione.
- Proteggere newsletter/discussione con una password - imposta una password che protegge l'accesso alla newsletter/discussione qualora qualcun altro si avvalga del client di posta elettronica o dei dati dell'account di un utente autorizzato.
- Aggiunta di iscritti all'elenco - aggiunge automaticamente utenti a newsletter/discussioni.

Creazione di un piè di pagina personalizzato per la lista



Schermata 68 - Proprietà del piè di pagina della newsletter

1. Fare clic con il pulsante destro del mouse sulla regola per aggiungere un piè di pagina e selezionare **Proprietà**.

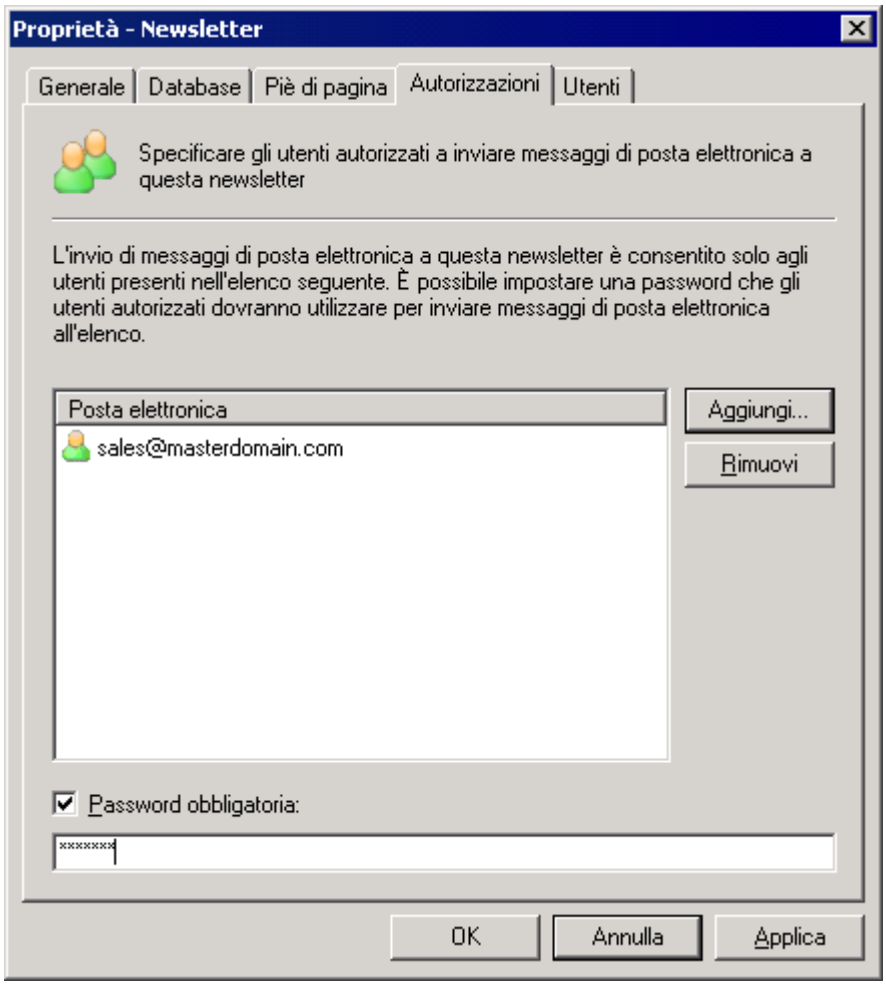
2. Nella scheda **Piè di pagina**, fare clic su **Modifica HTML** per creare un piè di pagina in formato HTML.

NOTA: si può adoperare il piè di pagina per informare gli utenti sulle modalità per iscriversi o cancellare l'iscrizione dall'elenco.

Impostazione delle autorizzazioni della lista

NOTA: le autorizzazioni non sono configurabili per le liste di discussione.

1. Fare clic con il pulsante destro del mouse sulla regola per impostare le autorizzazioni e selezionare **Proprietà**.



Schermata 69 - Impostazione delle autorizzazioni della newsletter

2. Nella scheda **Autorizzazioni**, fare clic sul pulsante **Aggiungi** e specificare gli utenti dotati di autorizzazioni a inviare un messaggio di posta elettronica all'elenco. Gli indirizzi di posta elettronica vengono aggiunti all'elenco di **Posta elettronica**.

3. È possibile impostare la password selezionando la casella di controllo **Password obbligatoria** e fornendo una password. Per maggiori informazioni sulla modalità di utilizzo di questa funzionalità, consultare la sezione successiva Proteggere newsletter con una password.

Proteggere newsletter con una password

NOTA: le liste di discussione non possono essere protette da password.

1. Fare clic con il pulsante destro del mouse sulla regola per impostare le autorizzazioni e selezionare **Proprietà**.

2. Nella scheda **Autorizzazioni**, selezionare la casella di controllo **Password obbligatoria:** e fornire una password.

IMPORTANTE: Si consiglia di consentire agli utenti di autenticarsi inviando essi stessi una password nell'oggetto del messaggio di posta elettronica al momento dell'invio di messaggi di posta elettronica alla newsletter. La password deve essere indicata nel campo dell'oggetto come segue:

[PASSWORD:<*password*>**]** <*L'oggetto del messaggio di posta elettronica!*>

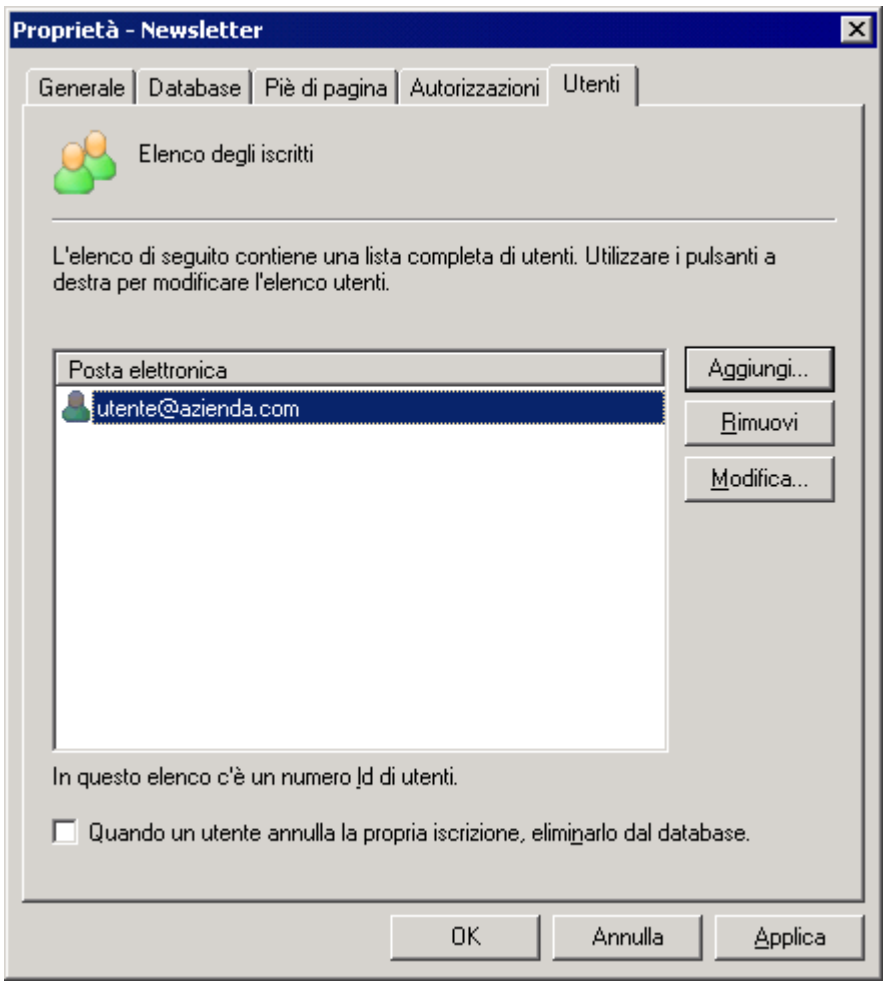
- **Esempio:** [PASSWORD:letmepost] Offerta Speciale.

Se la password è corretta, il server di elenco eliminerà i dati della password dall'oggetto e trasmetterà il messaggio di posta elettronica alla newsletter.

Aggiunta di iscritti alla lista

NOTA: si consiglia di consentire agli utenti di iscriversi espressamente alla lista, inviando essi stessi un messaggio di posta elettronica all'indirizzo di iscrizione della newsletter/discussione. Se si aggiungono degli utenti e non si è richiesta espressamente la loro autorizzazione, si potrebbero ricevere denunce di spam.

1. Fare clic con il pulsante destro del mouse sulla regola per impostare le autorizzazioni e selezionare **Proprietà**.



Schermata 70 - Inserimento di iscritti alla newsletter

2. Nella scheda **Iscritti**, fare clic sul pulsante **Aggiungi**.

3. Compilare i campi **Indirizzo di posta elettronica**, **Nome**, **Cognome** e **Azienda** e fare clic sul pulsante OK. L'indirizzo di posta elettronica del neoiscritto sarà aggiunto all'elenco **Posta elettronica**.

NOTA 1: i campi Nome, Cognome e Azienda sono facoltativi.

NOTA 2: selezionare l'utente e fare clic sul pulsante **Rimuovi** per

eliminare gli iscritti dalla lista.

NOTA 3: per rimuovere gli utenti dalla tabella della lista di iscrizione in caso di rinuncia all'iscrizione (e non limitarsi a etichettare l'utente come "non iscritto"), selezionare la casella di controllo **Elimina dal data base quando l'utente cancella l'iscrizione**.

4.5.3 Uso di newsletter/discussioni

Dopo aver creato una newsletter/lista di discussione, gli utenti devono iscriversi per poterla ricevere. Le azioni che gli utenti possono eseguire utilizzando le newsletter/discussioni sono le seguenti:

- inviare una newsletter
- iscriversi a una lista
- finalizzare la procedura di iscrizione
- inviare una newsletter
- annullare l'iscrizione a una lista

Uso di newsletter

- **Iscrizione alla lista** - chiede agli utenti di inviare un messaggio di posta elettronica a <nomenewsletter>-subscribe@dominioutente.com
- **Finalizzazione della procedura di iscrizione** - gli utenti inviano prima una richiesta di iscrizione a <nomenewsletter>-subscribe@dominioutente.com. Al ricevimento della richiesta, il server di elenco invia un messaggio di conferma. Gli utenti devono confermare la propria iscrizione rispondendo al messaggio di posta elettronica e accettando di essere aggiunti come iscritti.

  NOTA: il messaggio di posta elettronica di conferma è obbligatorio e non può essere annullato.
- **Invio di un messaggio/post di discussione alla newsletter** - i membri autorizzati a inviare messaggi alla lista devono inviare il messaggio di posta elettronica all'indirizzo della mailing list della newsletter.

  <nomenewsletter>@dominioutente.com
- **Annullamento dell'iscrizione alla lista** - per annullare l'iscrizione alla lista, gli utenti devono inviare un messaggio di posta elettronica a:

  <newslettername>-unsubscribe@yourdomain.com

Suggerimento: per consentire agli utenti di iscriversi facilmente alle newsletter, aggiungere un modulo Web con il quale si chiede il nome e l'indirizzo di posta elettronica e inviarne il risultato a:

<newslettername>-subscribe@yourdomain.com

4.5.4 Importazione di iscritti nella lista/nella struttura del data base

Quando si crea una nuova newsletter o una lista di discussionet, la procedura di configurazione crea una tabella denominata "*nomelista_iscritti*" contenente i campi descritti nella tabella di seguito riportata.

Se si desidera importare dati nella lista, è sufficiente accertarsi che il data base contenga i dati corretti nei campi corretti.

Nome campo	Tipo	Valore predefinito	Flag	Descrizione
Ls_id	Varchar(100)		PK	ID iscritto
Ls_first	Varchar(250)			Nome
Ls_last	Varchar(250)			Cognome
Ls_email	Varchar(250)			E-mail
Ls_unsubscribed	Int	0	NOT NULL	Annulla flag
ls_company	Varchar(250)			Nome azienda

5 Funzioni varie

Questa sezione descrive tutte le altre funzioni non previste nella configurazione iniziale, nella gestione quotidiana e nella personalizzazione di GFI MailEssentials. Tali funzioni comprendono:

- Configurazione dello scaricamento POP3
- Sincronizzazione dei dati di configurazione
- Selezione del server da cui scaricare gli aggiornamenti
- Selezione del server virtuale SMTP per il collegamento a GFI MailEssentials
- Comandi remoti

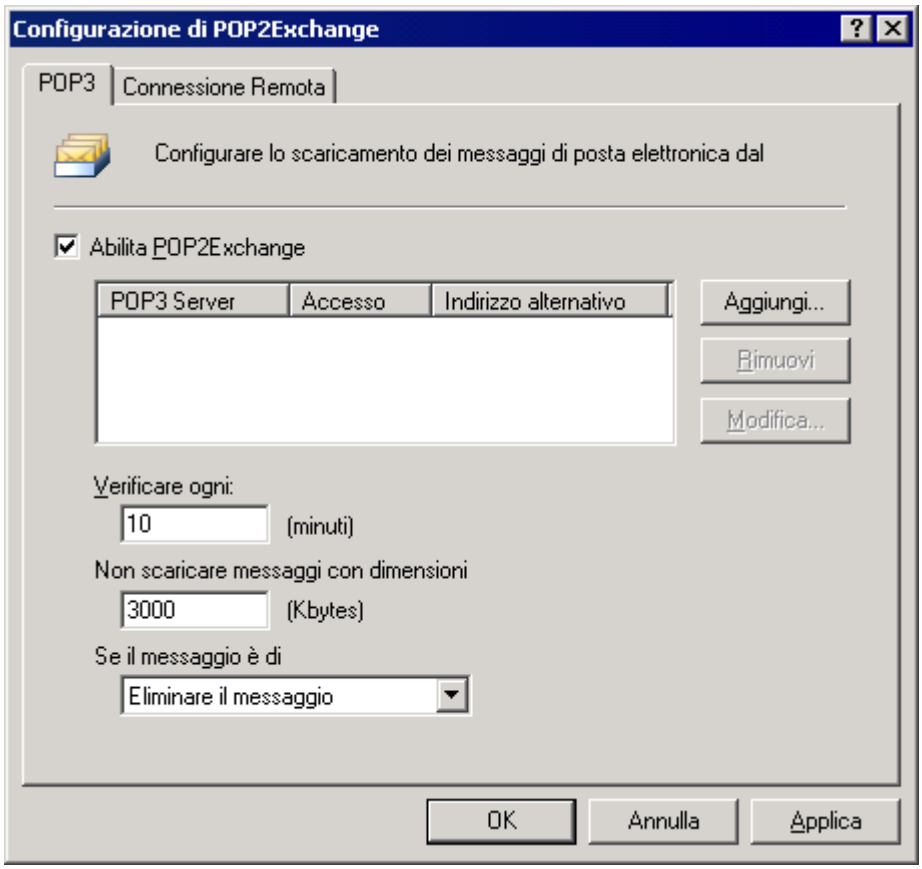
5.1 Configurazione del POP3 e scaricamento di connessione remota

Il Protocollo Ufficio Postale (POP3 (RFC 1225)) è un protocollo client/server per l'archiviazione dei messaggi di posta elettronica, tramite il quale il client può collegarsi al server POP3 e leggere la posta elettronica in qualsiasi momento. Un client di posta esegue una connessione TCP/IP con il server e, tramite lo scambio di una serie di comandi, consente all'utente di leggere la posta elettronica. Tutti gli ISP supportano il POP3.

Si consiglia di utilizzare il protocollo SMTP e di evitare il protocollo POP3 in quanto adatto all'acquisizione dei messaggi di posta elettronica unicamente per i client di posta elettronica, non per i server di posta. Tuttavia, considerando le situazioni in cui un indirizzo IP statico usato con SMTP non sia disponibile, GFI MailEssentials può usare POP3 per recuperare la posta elettronica.

5.1.1 Configurazione del *downloader* (programma di scaricamento) POP3

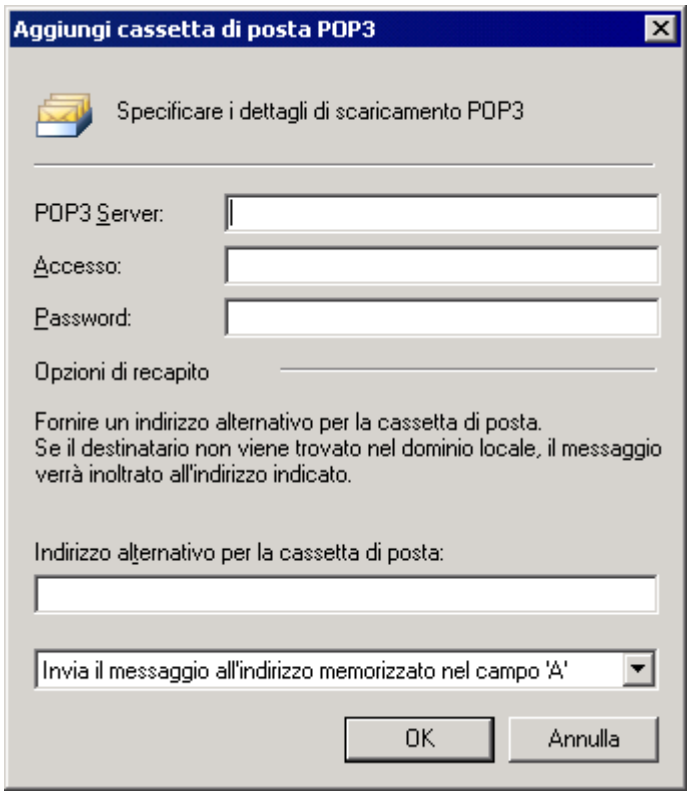
1. Selezionare il nodo **POP2Exchange** e fare doppio clic sulla voce **Generale**.



Schermata 71 - Downloader POP3 di GFI MailEssentials

2. Nella scheda **POP3**, selezionare la casella di controllo **Abilita POP2Exchange** per abilitare il downloader **POP3.**

3. Fare clic su **Aggiungi** per aggiungere una cassetta postale POP3 da cui scaricare la posta elettronica.



Schermata 72 - Aggiunta di una cassetta postale POP3

4. Inserire i dati del server POP3, il nome e la password di accesso della cassetta postale. È possibile scegliere tra:

- **Invia il messaggio all'indirizzo memorizzato nel campo "A" -** GFI MailEssentials analizza l'intestazione del messaggio e smista la posta di conseguenza. Se l'analisi del messaggio di posta elettronica ha esito negativo, il messaggio viene inviato all'indirizzo di posta elettronica alternativo specificato.
- **Invia messaggio all'indirizzo alternativo:** Tutti i messaggi di posta elettronica sono inoltrati da questa cassetta postale a un dato indirizzo di posta elettronica. Inserire l'indirizzo SMTP completo nel campo "Indirizzo di posta elettronica".
  - **Esempio:** john@company.com

5. Specificare quindi l'indirizzo alternativo e fare clic su **OK**.

NOTA 1: quando si specifica l'indirizzo di destinazione dei messaggi di posta elettronica (l'indirizzo al quale GFI MailEssentials inoltrerà i messaggi), accertarsi di aver impostato un indirizzo SMTP corrispondente sul server di posta in uso.

NOTA 2: è possibile configurare cassette postali POP3 multiple.

6. Nella finestra di dialogo di configurazione POP2Exchange, configurare altre opzioni disponibili.

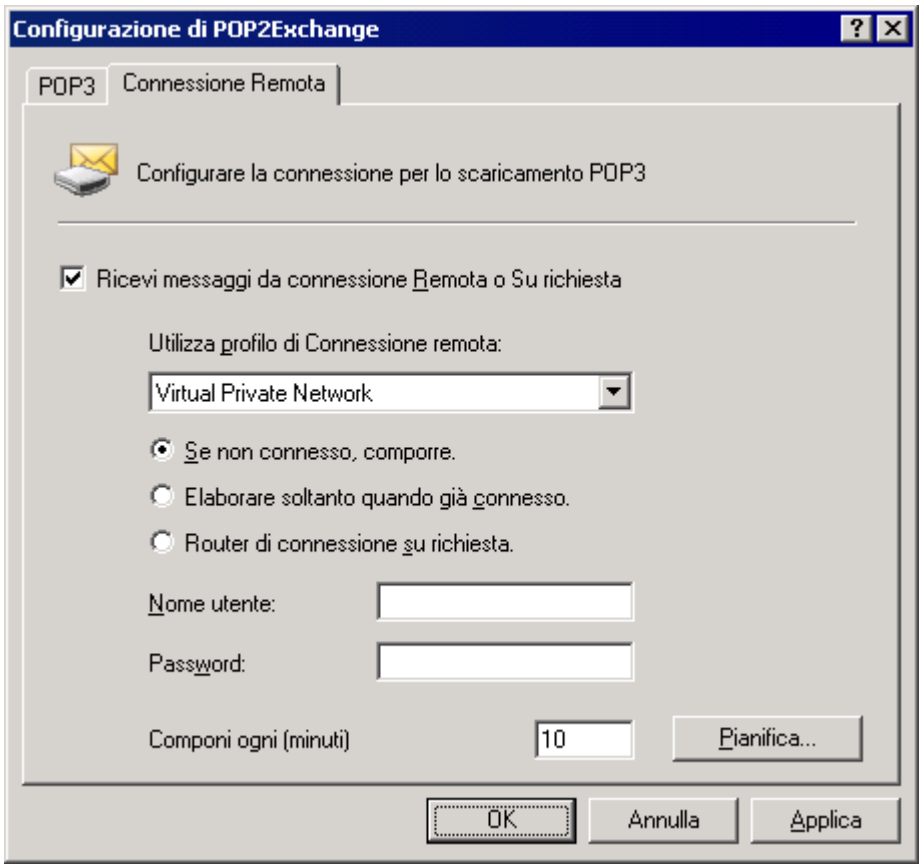
- **Controlla ogni (minuti):** indicare l'intervallo temporale di scaricamento.
- **Non scaricare messaggi con dimensioni superiori a (Kbytes):** specificare la dimensione massima dello scaricamento. Se supera questo limite, il messaggio di posta elettronica non viene scaricato.
- **Se il messaggio è di dimensioni superiori:** scegliere di

eliminare il messaggio di posta elettronica di dimensioni superiori al limite massimo consentito oppure inviare un messaggio al *postmaster*.

5.1.2 Configurazione delle opzioni di connessione remota

1. Selezionare il nodo **POP2Exchange** e fare doppio clic sulla voce **Generale**.

2. Dalla scheda **Connessione remota**, selezionare la casella di controllo **Ricevi messaggi da connessione remota o Su richiesta** per abilitare la connessione remota.



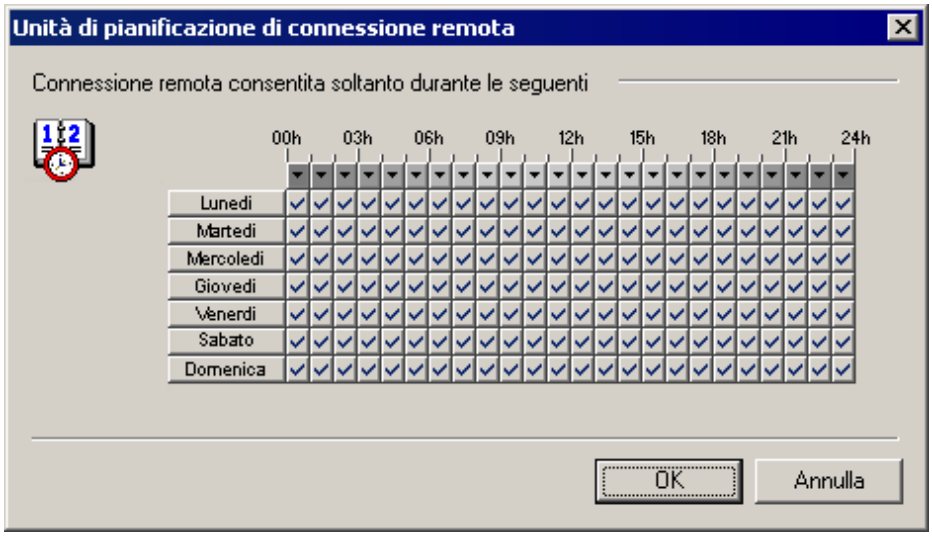
Schermata 73 - Opzioni di connessione remota

3. Selezionare un profilo di Connessione remota, un nome e una password di accesso. Sono disponibili le seguenti opzioni:

- **Utilizza profilo di Connessione remota:** Scegliere il profilo di Connessione remota che si desidera adoperare.
- **Se non connesso, comporre:** GFI MailEssentials chiama soltanto se non è presente alcuna connessione.
- **Nome utente:** inserire il nome utente utilizzato per accedere al proprio ISP.
- **Password:** inserire la password utilizzata per accedere al proprio ISP.
- **Elaborare soltanto quando già connesso:** GFI MailEssentials elabora il messaggio di posta elettronica soltanto se esiste già una connessione.
- **Router di connessione su richiesta:** selezionare questa opzione

se si dispone di un router con connessione a Internet di tipo *Dial On Demand* (su richiesta). GFI MailEssentials acquisisce i messaggi di posta elettronica negli intervalli specificati, ma senza abilitare una connessione remota.

- **Elabora ogni (minuti):** inserire l'intervallo temporale in cui GFI MailEssentials deve effettuare la connessione remota oppure verificare se esiste una connessione (dipende se si è impostato GFI MailEssentials affinché effettui le connessioni remote oppure soltanto affinché elabori i messaggi di posta elettronica quando si è già connessi).



Schermata 74 - Configurazione del periodo in cui GFI MailEssentials deve acquisire i messaggi di posta elettronica

4. Fare clic su **Pianifica** e indicare le ore in cui GFI MailEssentials deve effettuare la connessione remota per acquisire i messaggi di posta elettronica. Il segno di spunta indica che GFI MailEssentials effettuerà la connessione. Il segno "X" indica che GFI MailEssentials non effettuerà la connessione all'ora indicata.

5. Fare clic su **OK** per completare la configurazione.

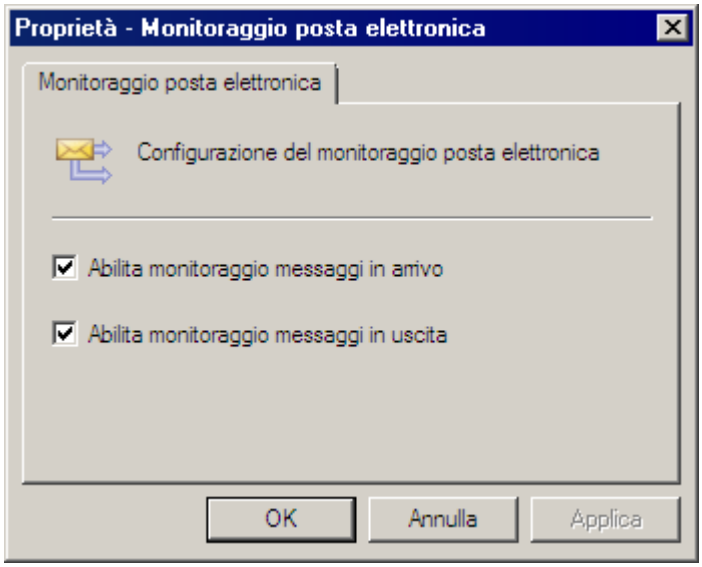
5.2 Monitoraggio dei messaggi di posta elettronica

La funzionalità di monitoraggio dei messaggi di posta elettronica consente di trasmettere una copia dei messaggi inviati o ricevuti da un dato indirizzo di posta elettronica a un altro indirizzo di posta elettronica, consentendo di mantenere un archivio a livello centrale delle comunicazioni di posta elettronica di un particolare soggetto o di un reparto specifico.

Questa funzionalità può essere usata anche come alternativa all'archiviazione dei messaggi di posta elettronica dal momento che tutti i messaggi possono essere inviati automaticamente in archivi di Microsoft Exchange Server o Microsoft Outlook.

5.2.1 Abilitazione o disabilitazione del monitoraggio dei messaggi di posta elettronica

1. Fare clic con il pulsante destro del mouse su **Gestione posta elettronica ► Monitoraggio posta elettronica** e selezionare **Proprietà**.



Schermata 75 - Abilitazione o disabilitazione del monitoraggio dei messaggi di posta elettronica

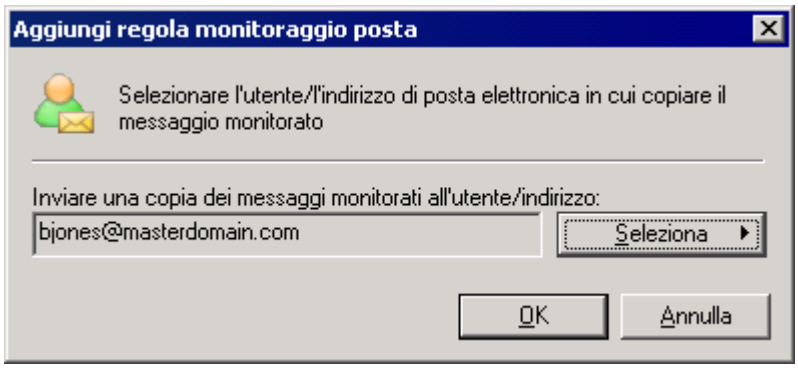
2. Per abilitare/disabilitare tutte le regole di monitoraggio dei messaggi di posta elettronica in arrivo o in uscita, selezionare/deselezionare le caselle di controllo **Abilita monitoraggio messaggi in arrivo** e **Abilita monitoraggio messaggi in uscita.**

3. Fare clic sul pulsante **OK** per salvare le modifiche.

NOTA: per abilitare/disabilitare una singola regola di monitoraggio dei messaggi di posta elettronica, fare clic con il pulsante destro del mouse sulla regola di monitoraggio dei messaggi di posta elettronica e selezionare **Abilita/Disabilita**.

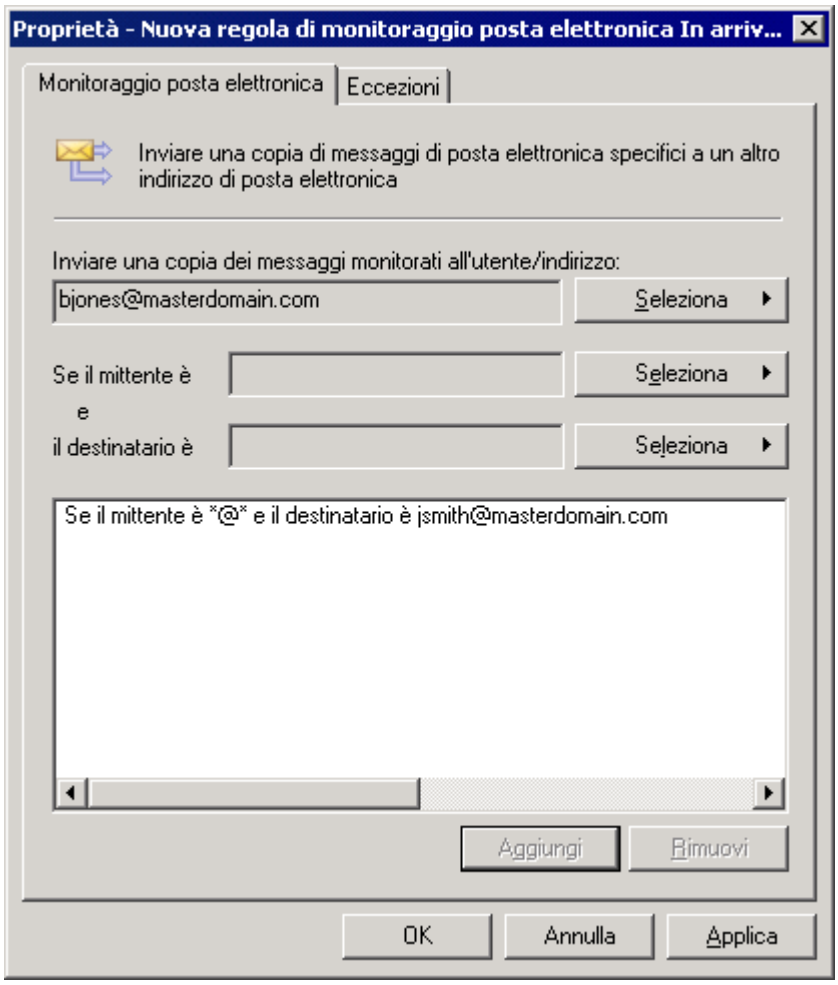
5.2.2 Configurazione del monitoraggio dei messaggi di posta elettronica

1. Fare clic con il pulsante destro del mouse sul nodo **Gestione posta elettronica ► Monitoraggio posta elettronica** e selezionare **Nuovo ► Regola di monitoraggio posta in arrivo** o **Regola di monitoraggio posta in uscita** per monitorare, rispettivamente, la posta elettronica in arrivo o in uscita.



Schermata 76 - Aggiunta della regola di monitoraggio della posta

2. Inserire l'indirizzo di posta elettronica di destinazione o la cassetta postale verso cui copiare i messaggi di posta elettronica. Fare clic su **OK** per continuare.

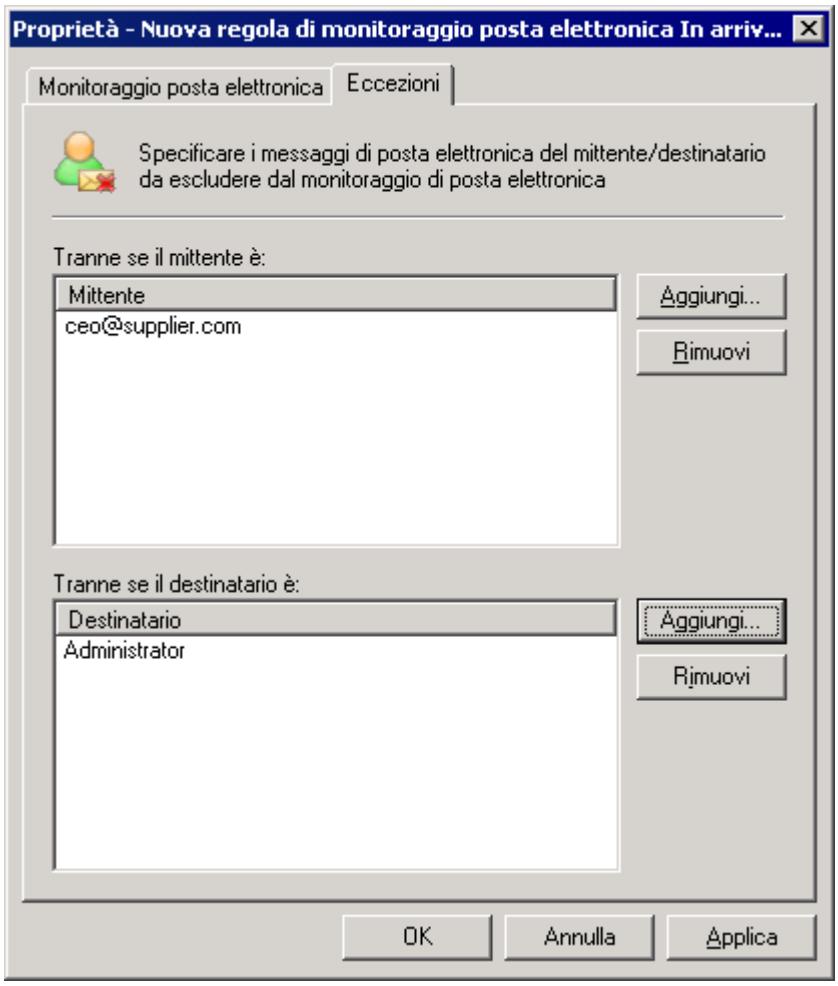


Schermata 77 - Configurazione del monitoraggio dei messaggi di posta elettronica

3. Fare clic sui pulsanti **Seleziona** accanto a Mittente e Destinatario per indicare quali messaggi di posta elettronica devono essere monitorati da questa regola. Fare clic su **Aggiungi** per aggiungere filtri a questo elenco. Ripetere questa procedura per specificare più filtri. È possibile monitorare le seguenti condizioni:

NOTA: per monitorare tutta la posta, inserire *@*.

- **Tutti i messaggi di posta elettronica inviati da un particolare utente** - creare la regola di uscita e indicare il messaggio di posta del mittente o selezionare l'utente (se si utilizza AD) nel campo del mittente e inserire*@* come dominio del destinatario.
- **Tutti i messaggi di posta elettronica inviati a un particolare utente** - creare la regola di entrata e indicare il messaggio di posta del destinatario o selezionare l'utente (se si utilizza AD) nel campo del destinatario e specificare*@* come dominio del mittente.
- **Messaggi di posta elettronica inviati da un particolare utente a un destinatario esterno** - creare una regola di uscita e indicare il mittente o selezionare l'utente (se si utilizza AD) nel campo del mittente. Inserire quindi l'indirizzo di posta elettronica del destinatario nel campo del destinatario.
- **Messaggi di posta elettronica inviati da un mittente esterno a un particolare utente** - creare una regola di entrata e indicare l'indirizzo di posta elettronica del mittente esterno nel campo del mittente. Inserire quindi il nome o l'indirizzo di posta elettronica dell'utente nel campo del destinatario.
- **Messaggi di posta elettronica inviati da un particolare utente a un'azienda o a un dominio**- creare una regola di uscita e indicare il mittente o selezionare l'utente (se si utilizza AD) nel campo del mittente. Specificare quindi il dominio dell'azienda nel campo del destinatario, selezionando **Dominio** con il pulsante **Destinatario**.
- **Messaggi di posta elettronica inviati a un particolare utente da un'azienda o da un dominio** - creare una regola di entrata e indicare il dominio dell'azienda nel campo del mittente. A questo scopo, quando si fa clic sul pulsante **Mittente**, selezionare **Dominio**. Inserire quindi il nome o l'indirizzo di posta elettronica dell'utente nel campo del destinatario.



Schermata 78 - Creare un'eccezione

4. Selezionare la scheda Eccezioni per escludere mittenti o destinatari dalla nuova regola. Le opzioni disponibili sono:

- **Tranne se il mittente è** - Esclude il mittente indicato dall'elenco.
- **Tranne se il destinatario è** - Esclude il destinatario indicato dall'elenco.

NOTA 1: quando si indicano le eccezioni per la regola di monitoraggio della posta in arrivo, l'elenco **Mittente** contiene indirizzi di posta elettronica non locali e l'elenco **Destinatario** contiene tutti gli indirizzi locali. Quando si indicano le eccezioni per la regola di monitoraggio della posta in uscita, l'elenco **Mittente** contiene indirizzi di posta elettronica locali e l'elenco **Destinatario** contiene solamente indirizzi non locali.

NOTA 2: si applicano entrambi gli elenchi eccezioni e non saranno controllati tutti i mittenti compresi nell'elenco delle eccezioni del mittente né tutti i destinatari compresi nell'elenco dei destinatari..

5. Fare clic su **OK** per completare le impostazioni.

NOTA: per attribuire alla nuova regola di monitoraggio dei messaggi di posta elettronica un nuovo nome, fare clic sulla regola di monitoraggio della posta e premere il tasto F2.

5.3 Sincronizzazione dei dati di configurazione

Se si è installato GFI MailEssentials su più di un server, si desidera probabilmente sincronizzare l'antispam e i dati di configurazione generali tra i vari server, di modo che i messaggi di posta elettronica individuati come spam da un server siano considerati tali anche da un altro server, nell'eventualità che essi attraversino quest'ultimo server.

GFI MailEssentials rende automatica questa procedura mediante due funzionalità che mantengono sincronizzate le varie installazioni di GFI MailEssentials.

- Anti-spam Synchronization Agent: questo servizio cura la sincronizzazione delle impostazioni antispam tra le installazioni di GFI MailEssentials avvalendosi del servizio Microsoft BITS.

  Anti-spam Synchronization Agent (agente di sincronizzazione antispam) funziona con le seguenti modalità:

  1. Il computer server che ospita GFI MailEssentials è configurato come il server master.

  2. Gli altri computer server sui cui è installato GFI MailEssentials sono configurati come server slave.

  3. I server slave caricano un file di archivio, contenente le impostazioni antispam, su una cartella IIS virtuale ospitata sul server master mediante il servizio BITS.

  4. Quando il server master ha raccolto tutti i dati antispam dai server slave, i dati vengono estratti dai loro archivi singoli e uniti in un nuovo file di archivio delle impostazioni antispam aggiornato.

  5. I server slave scaricano questo file di archivio di impostazioni antispam aggiornato, ne estraggono il contenuto e aggiornano l'installazione GFI MailEssentials locale per poter adoperare le nuove impostazioni.

  NOTA 1: i server che partecipano alla sincronizzazione delle impostazioni antispam devono avere tutti GFI MailEssentials 14.1 installato.

  NOTA 2: i file caricati e scaricati da Anti-spam Synchronization Agent sono costituiti da archivi compressi per limitare il traffico sulla rete.

  Consultare la sezione Anti-spam Synchronization Agent Configuration a pagina 112 del presente manuale per maggiori informazioni sulla modalità di configurazione di Anti-spam Synchronization Agent.

- GFI MailEssentials Configuration Export/Import ToolL'applicazione di esportazione e importazione di tutte le impostazioni di GFI MailEssentials configuration consente di configurare una nuova installazione di GFI MailEssentials con le stesse identiche impostazioni di un'altra installazione già operativa e funzionante.

5.3.1 Anti-spam Synchronization Agent Configuration

La configurazione di richiede di seguire le seguenti fasi nell'ordine descritto in basso:

Fase 1: configurazione del server master

Fase 2: installazione dell'estensione server BITS sul server master

Fase 3: configurazione del server slave

5.3.2 Configurazione del server master

Note importanti

1. È possibile configurare come server master un solo server per volta.

2. Per configurare un server come server master, deve soddisfare una delle seguenti specifiche di sistema:

- Microsoft Windows 2003 con SP1 o successivi e IIS6.0 con installata l'estensione server BITS (ulteriori informazioni sulle modalità per installare l'estensione server BITS sono riportate di seguito).
- Microsoft Windows 2000 con SP3 o successivi e IIS5.0 con installata l'estensione server BITS (ulteriori informazioni sulle modalità per installare l'estensione server BITS sono riportate di seguito).

NOTA: un computer Microsoft Windows XP non può essere configurato come master in quanto non supporta l'estensione server Microsoft BITS.

Configurazione del server master

1. Installare l'estensione server Microsoft BITS. Per maggiori informazioni, consultare la sezione Installazione dell'estensione server BITS sul server master a pagina 87 del presente manuale.

2. Dal gruppo Strumenti amministrativi, caricare la console **Internet Information Services (IIS) Manager**, fare clic con il pulsante destro del mouse sul sito Web di propria scelta e selezionare **Nuovo ► Directory virtuale** dal menu di scelta rapida.

3. Seguire le fasi della **Procedura guidata Creazione directory virtuale** e creare la nuova directory virtuale.

NOTA: accertarsi che solamente le caselle di controllo **Lettura** e **Scrittura** siano abilitate e che tutte le altre caselle di controllo siano deselezionate.

4. Fare clic con il pulsante destro del mouse sulla nuova directory virtuale e selezionare **Proprietà**. Selezionare la scheda **Protezione directory** e fare clic su **Modifica** situato nel gruppo **Controllo autenticazione e accesso**.

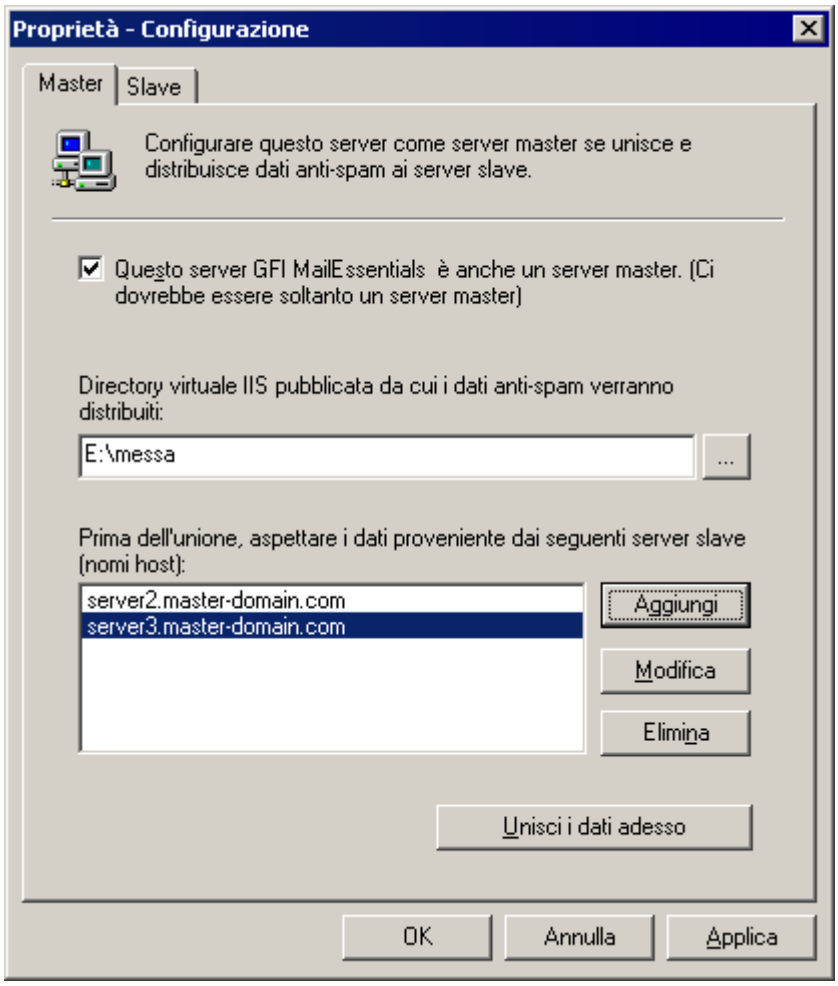
5. Selezionare la casella di controllo **Autenticazione di base** e specificare il Dominio predefinito e **Realm** a cui appartengono il nome utente e la password usati per l'autenticazione dai computer slave.

NOTA: accertarsi che tutte le altre caselle di controllo siano deselezionate.

6. Fare clic su **OK** e chiudere la finestra di dialogo **Metodi di autenticazione**.

7. Accedere alla scheda **Estensione server BITS** e selezionare la casella di controllo **Consenti ai client di trasferire i dati a questa directory virtuale**.

8. Selezionare **Start ► GFI MailEssentials ► GFI MailEssentials - Agente di sincronizzazione anti-spam**, fare clic con il pulsante destro del mouse sul nodo **Configurazione** e selezionare **Proprietà**.



Schermata 79- Configurazione di un server master

9. Dalla scheda **Master,** selezionare la casella di controllo **Questo server GFI MailEssentials è anche un server master** e inserire l'intero percorso della cartella configurata per conservare i contenuti della directory virtuale.

10. Fare clic sul pulsante **Aggiungi** e inserire l'*hostname* del server slave nella casella di modifica **Server**. Fare clic su **OK** per aggiungerlo all'elenco. Ripetere questa fase per aggiungere tutti gli altri server slave configurati.

NOTA 1: accertarsi di configurare tutti i computer aggiunti all'elenco di server slave. Diversamente, lo slave sul server master non unirà i dati.

NOTA 2: è possibile configurare il master contemporaneamente anche come slave. Pertanto, il server confluirà i propri dati sulle impostazioni antispam a quelli caricati dagli altri server slave. In questo caso, è necessario aggiungere anche l'*hostname* del server master all'elenco dei server slave. Per maggiori informazioni, consultare il capitolo Configurazione di un server slave a pagina 87 del presente manuale.

11. Se richiesto, selezionare un server slave dall'elenco e fare clic sul pulsante **Modifica** o **Elimina** per modificarlo o eliminarlo.

12. Fare clic sul pulsante **OK** per salvare le impostazioni.

5.3.3 Installazione dell'estensione server BITS sul server master

1. Scaricare BITS v1.5 Server Component Microsoft dal seguente link ed eseguirlo sul server master:

http://www.microsoft.com/downloads/details.aspx?FamilyID=17967848-be86-4cd6-891c-ec8241611ad4&displaylang= it

2. Seguire le istruzioni della **Procedura guidata del Server BITS** per completare l'installazione.

3. Dal **Pannello di controllo** caricare **Aggiungi o rimuovi programmi** e selezionare la scheda **Aggiungi/Rimuovi componenti di Windows**.

4. Dalla finestra di dialogo **Procedura guidata componenti di Windows**, selezionare **Server applicazioni** dall'elenco **Componenti** e fare clic su **Dettagli**.

4. Dalla finestra di dialogo **Server applicazioni**, selezionare **Internet Information Services (IIS) nell'elenco Subcomponenti del server applicazioni e fare clic su Dettagli.**

5. Selezionare la casella di controllo **Estensione server Background Intelligent Transfer Service (BITS)** dall'elenco **Subcomponenti di Internet Information Services (IIS)** e fare clic sul pulsante **OK**.

6. Fare clic su **OK** per chiudere la finestra di dialogo **Server applicazioni**.

7. Dalla finestra di dialogo **Procedura guidata componenti di Windows**, fare clic sul pulsante **Avanti** per avviare l'installazione.

8. Al termine, fare clic su Fine per chiudere **Procedura guidata componenti di Windows.**

5.3.4 Configurazione di un server slave

Note importanti

Per configurare un server come server slave, deve soddisfare una delle seguenti specifiche di sistema:

- Microsoft Windows 2003. Si consiglia di scaricare l'aggiornamento client BITS 2.0 dal seguente link Microsoft:

  http://www.microsoft.com/downloads/details.aspx?familyid=3FD31F05-D091-49B3-8A80-BF9B83261372&displaylang=it

- Microsoft Windows 2000 con SP3 o successivi. È necessario scaricare e installare il client BITS 2.0 dal seguente link Microsoft:

  http://www.microsoft.com/downloads/details.aspx?FamilyID=3ee866a0-3a09-4fdf-8bdb-c906850ab9f2&DisplayLang=it

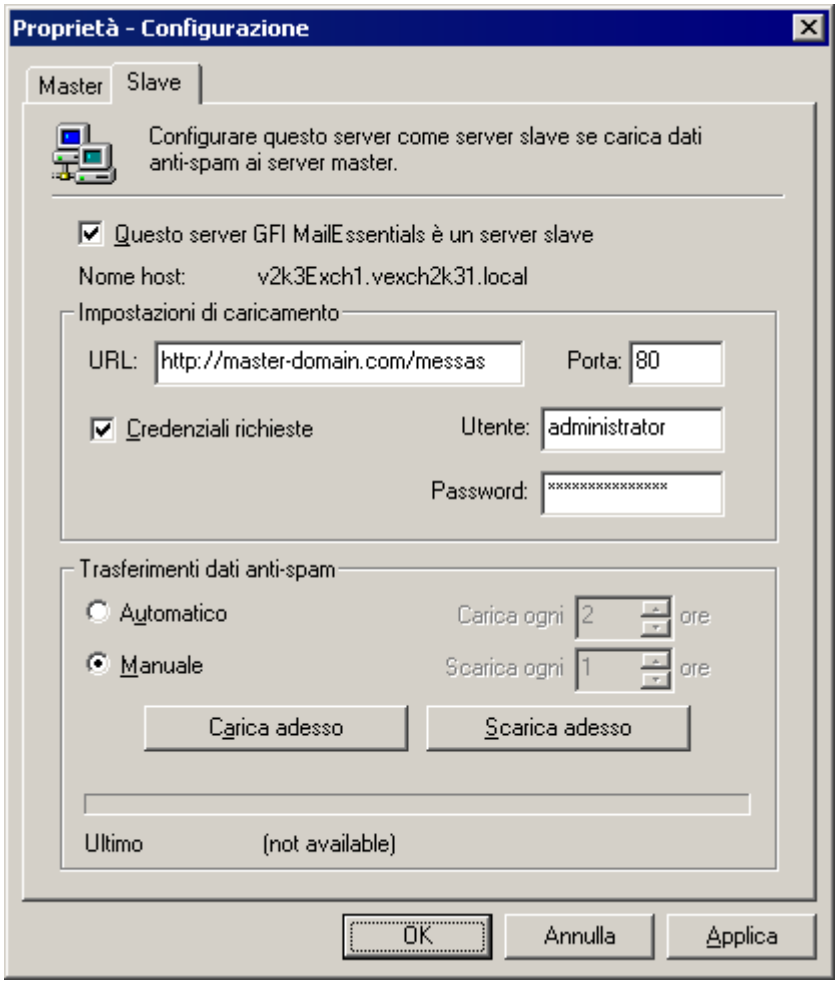
- Microsoft Windows XP Professional. È necessario scaricare e installare il client BITS 2.0 dal seguente link Microsoft:

  http://www.microsoft.com/downloads/details.aspx?FamilyID=b93356b1-ba43-480f-983d-eb19368f9047&DisplayLang=it

Configurazione del server slave

1. Fare clic su **Start ► GFI MailEssentials ► GFI MailEssentials - Agente di sincronizzazione anti-spam.**

2. Fare clic con il pulsante destro del mouse sul nodo ► **Configurazione** e selezionare **Proprietà**.



Schermata 80 - Configurazione di un server slave

3. Dalla scheda Slave, selezionare la casella di controllo **Questo server GFI MailEssentials è un server slave** e indicare l'intero URL della directory virtuale ospitata sul server master nel campo **URL**.

- **Esempio:** "http://master-domain.com/messas"

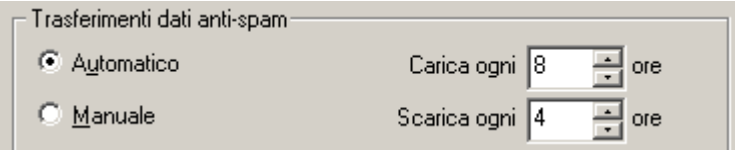
4. Nel campo **Porta**, specificare la porta su cui il server master accetta le comunicazioni HTTP.

NOTA: la porta è impostata in modo predefinito sulla porta standard adoperata per HTTP, cioè la porta 80.

5. Selezionare la casella di controllo **Credenziali richieste** e inserire il nome utente/la password usati per autenticarsi sul server master.

6. Selezionare:

- **Manuale** - per caricare e scaricare il file di archivio delle impostazioni antispam manualmente. Per caricare le impostazioni antispam del server slave sul server master, è necessario fare clic sul pulsante **Carica adesso**. Per scaricare le impostazioni antispam confluite aggiornate dal server master, è necessario fare clic sul pulsante **Scarica adesso**.



Schermata 81 - Impostazione intervallo orario di caricamento/scaricamento

- **Automatico** - per configurare la sincronizzazione antispam automatica. Nel campo **Carica ogni**, indicare l'intervallo di caricamento espresso in ore, il che determina la frequenza con la quale il server slave carica le proprie impostazioni antispam sul server master. Nel campo **Scarica ogni**, indicare l'intervallo di scaricamento espresso in ore, il che determina la frequenza con la quale il server slave controlla gli aggiornamenti sul server master e li scarica se presenti.

NOTA: l'intervallo orario per caricare e scaricare non può essere impostato sulla stessa ora. Tale intervallo orario può essere impostato su qualsiasi valore compreso tra 1 e 240 ore. Si consiglia di configurare l'intervallo di scaricamento su un valore inferiore a quello dell'intervallo di caricamento e di impostare lo stesso intervallo temporale per tutti i server slave configurati.

- **Esempio:** Se l'intervallo di scaricamento è impostato su 3 ore, quello di caricamento deve essere impostato su 4 ore. In questo modo gli scaricamenti sono più frequenti dei caricamenti.

7. Fare clic sul pulsante **OK** per salvare le impostazioni.

5.4 GFI MailEssentials configuration Export/Import tool

Configuration Export/Import tool (strumento di esportazione e importazione della configurazione) richiede che le seguenti fasi siano eseguite nell'ordine riportato di seguito:

Fase 1: Esportazione delle impostazioni di GFI MailEssentials configuration

Fase 2: Copiare manualmente le impostazioni esportate sul computer dove è stato installato di recente GFI MailEssentials.

Fase 3: Importazione delle impostazioni di installazione di GFI MailEssentials

IMPORTANTE: quando si importano le impostazioni, vengono sovrascritte le impostazioni d'installazione di GFI MailEssentials correnti.

5.4.1 Esportazione delle impostazioni di GFI MailEssentials configuration

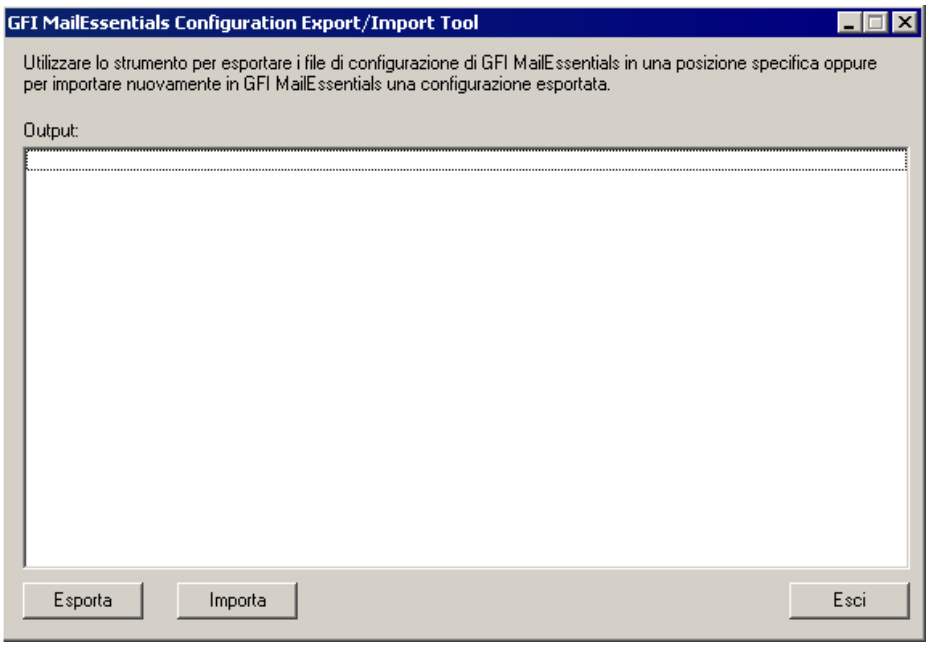
Per esportare le impostazioni di configurazione, procedere con i due metodi seguenti:

Esportazione mediante l'interfaccia dell'utente

Esportazione delle impostazioni mediante la linea di comando

Esportazione mediante l'interfaccia dell'utente

1. Fare doppio clic su "meconfigmgr.exe", situato nella cartella di root dell'installazione di GFI MailEssentials.



Schermata 82 -GFI MailEssentials configuration Export/Import tool

2. Fare clic sul pulsante **Esporta**. Nella finestra di dialogo **Cerca cartella**, scegliere la cartella per esportare le impostazioni di GFI MailEssentials configuration e fare clic su **OK**.

3. Al termine, fare clic sul pulsante **Esci**.

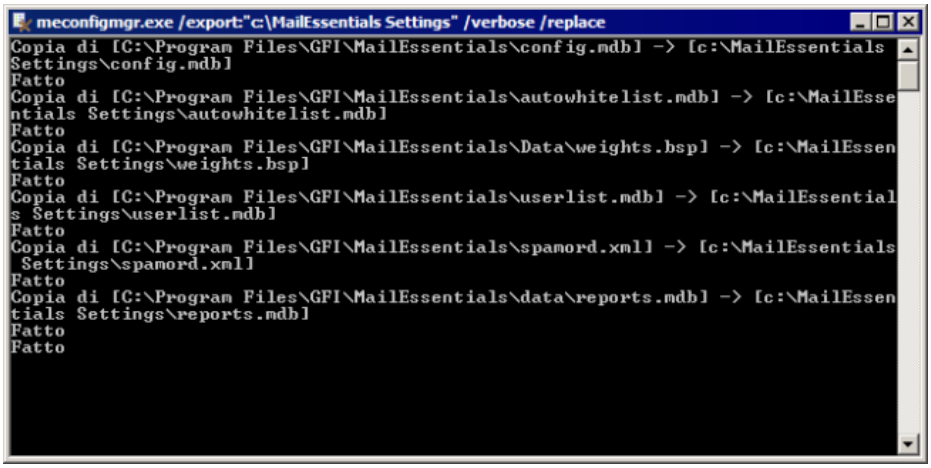
Esportazione delle impostazioni mediante la linea di comando

1. Dalla finestra di comando, cercare la cartella di root dell'installazione di GFI MailEssentials.

2. Inserire:

```
meconfigmgr /export:"c:\MailEssentials Settings" /verbose /replace
```

NOTA: sostituire "C:\MailEssentials Settings" con il percorso di destinazione desiderato.



Schermata 83 - Esportazione delle impostazioni mediante la linea di comando

Lo switch /verbose ordina allo strumento di visualizzare lo stato di avanzamento durante la copia dei file.

Lo switch /replace ordina allo strumento di sovrascrivere i file esistenti nella cartella di destinazione.

5.4.2 Importazione delle impostazioni di GFI MailEssentials configuration

Per importare le impostazioni di configurazione con GFI MailEssentials, procedere con i due metodi seguenti:

- Mediante l'interfaccia utente di GFI MailEssentials configuration Export/Import tool
- Mediante la linea di comando di GFI MailEssentials Configuration Export/Import tool

Importazione mediante l'interfaccia dell'utente

1. Fare doppio clic su "meconfigmgr.exe", situato nella cartella di root dell'installazione di GFI MailEssentials.

2. Fare clic sul pulsante **Importa**, scegliere la cartella che contiene le impostazioni di GFI MailEssentials configuration esportate e fare clic su **OK**.

3. Al termine, fare clic sul pulsante **Esci**.

Importazione mediante la linea di comando

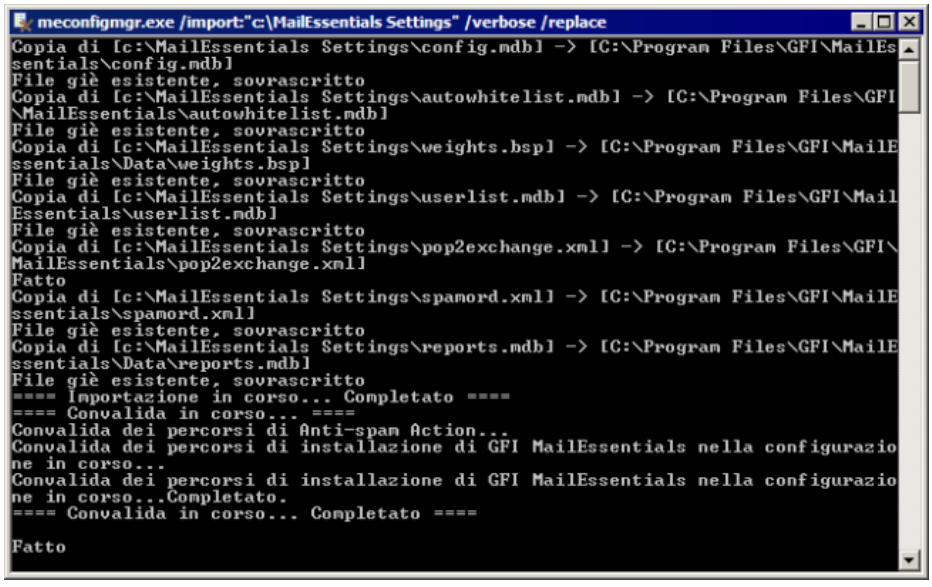
1. Arrestare i servizi IIS Admin e GFI MailEssentials Managed Attended eseguendo 'services.msc' e terminando i servizi.

2. Dalla finestra di comando, cercare la cartella di root dell'installazione di GFI MailEssentials.

3. Inserire:

```
meconfigmgr /import:"c:\MailEssentials Settings" /verbose /replace
```

Nota: sostituire "C:\MailEssentials Settings" con il percorso di fonte desiderato.



Schermata 84 - Importazione delle impostazioni mediante la linea di comando

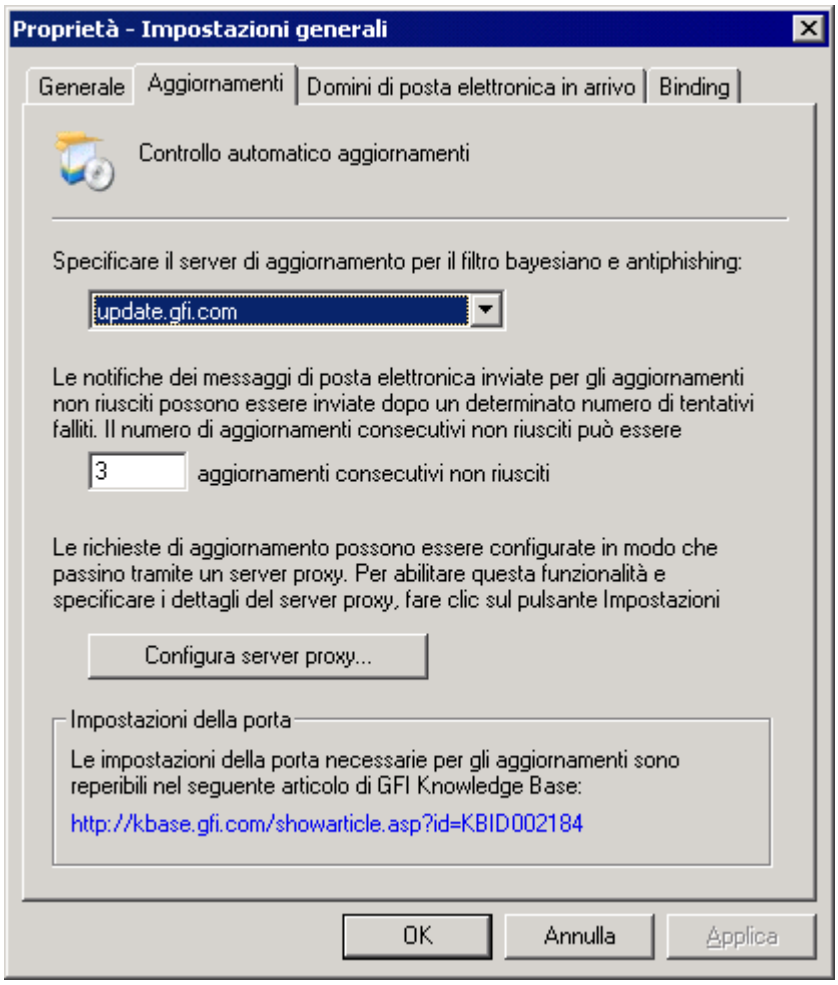
- Lo switch /verbose ordina allo strumento di visualizzare lo stato di

avanzamento durante la copia dei file come illustrato nella schermata seguente.

- Lo switch /replace ordina allo strumento di sovrascrivere i file esistenti nella cartella di destinazione.

5.5 Configurazione aggiornamenti automatici

GFI MailEssentials può essere configurato per la verifica e lo scaricamento automatici degli aggiornamenti.



Schermata 9 - Configurazione aggiornamenti automatici

1. Per configurare gli aggiornamenti automatici fare clic con il pulsante destro del mouse sul nodo **Generale**, selezionare **Proprietà** e fare clic sulla scheda **Aggiornamenti**.

- Specificare il server degli aggiornamenti usato per verificare e scaricare gli aggiornamenti del filtro antispam bayesiano e gli aggiornamenti antiphishing.
- Specificare il numero di aggiornamenti consecutivi non riusciti prima che sia inviato un messaggio di notifica.
- Per scaricare gli aggiornamenti con un server proxy fare clic su **Configura server proxy…**. Specificare le impostazioni del server proxy nella finestra di dialogo Impostazioni proxy.

2. Fare clic su **OK** per completare la configurazione.

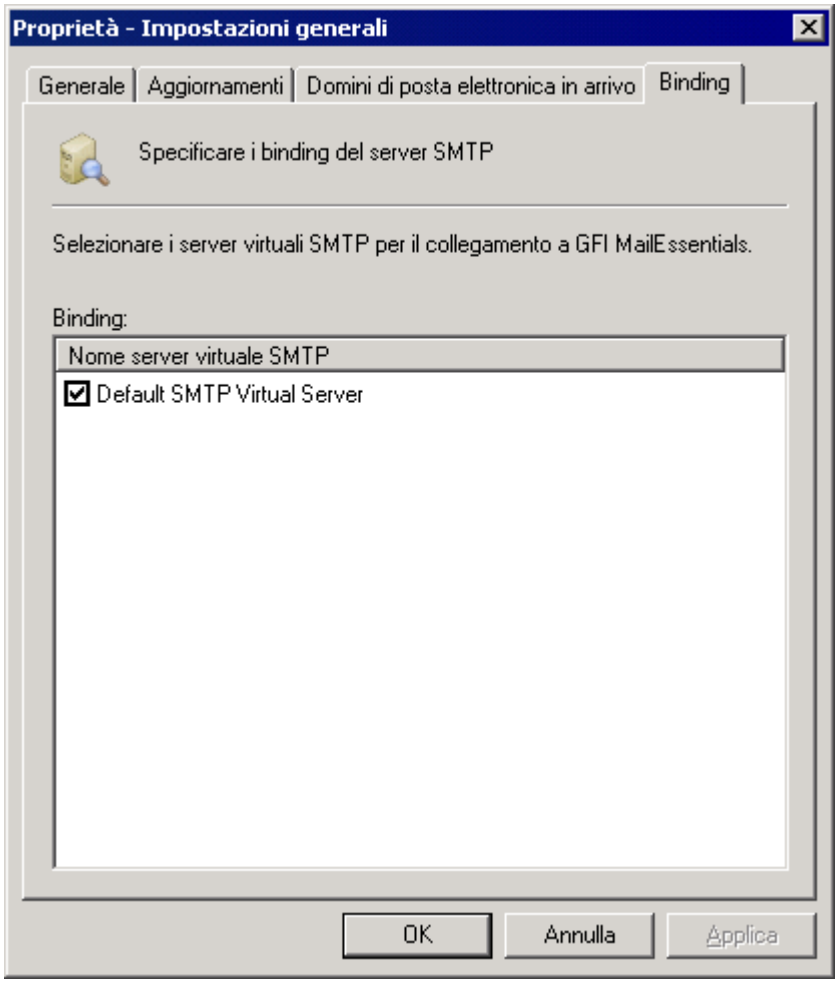
5.6 Selezione del server virtuale SMTP per il collegamento a GFI MailEssentials

In caso di server virtuali SMTP multipli, potrebbe essere necessario collegare GFI MailEssentials a nuovi o diversi server virtuali SMTP.

NOTA: la scheda **Binding** del server virtuale SMTP non viene visualizzata se GFI MailEssentials è stato installato su un computer avente Microsoft Exchange Server 2007/2010.

5.6.1 Collegamento tra GFI MailEssentials e i server virtuali SMTP

1. Fare clic con il pulsante destro del mouse sul nodo **Generale**, selezionare **Proprietà** e fare clic sulla scheda **Binding**.



Schermata 86 - Binding del server virtuale SMTP

2. Dall'elenco **Nome del server virtuale SMTP**, selezionare la casella di controllo del server virtuale SMTP a cui collegare GFI MailEssentials.

3. Fare clic sul pulsante **OK** per completare la configurazione.

NOTA: GFI MailEssentials configuration richiederà il riavvio dei servizi come il servizio SMTP IIS affinché abbiano effetto le nuove impostazioni. Fare clic sul pulsante **Sì** per riavviare i servizi.

5.7 Comandi remoti

I comandi remoti agevolano l'aggiunta di domini o indirizzi di posta elettronica alla black list di spam e l'aggiornamento del filtro bayesiano con messaggi di spam o ham (validi).

I comandi remoti funzionano mediante l'invio di un messaggio di posta elettronica a GFI MailEssentials: Con il semplice invio di un messaggio di posta elettronica a rcommands@mailessentials.com (configurabile), GFI MailEssentials riconosce il messaggio di posta elettronica come contenente comandi remoti e procede con la loro elaborazione.

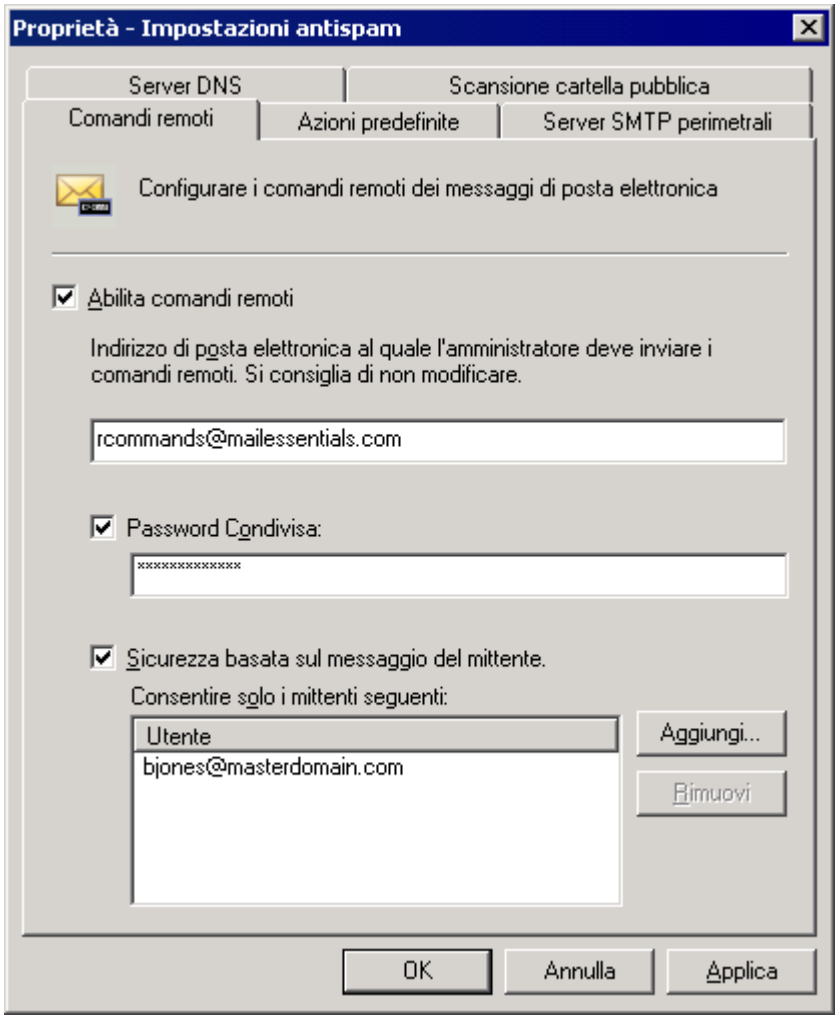
Con i comandi remoti è possibile:

1. Aggiungere spam o ham al modulo bayesiano.

2. Aggiungere parole chiave alla caratteristica di controllo parole chiave contenute nell'oggetto oppure nel testo del messaggio.

3. Aggiungere indirizzi di posta elettronica alla caratteristica della black listlist.

5.7.1 Configurazione dei comandi remoti



Schermata 87 - Comandi remoti

1. Fare clic con il pulsante destro del mouse su **Antispam** ► **Impostazioni antispam**, selezionare **Proprietà**, fare clic sulla scheda

Comandi remoti e selezionare la casella di controllo **Abilita comandi remoti**.

2. È possibile modificare l'indirizzo di posta elettronica cui inviare i comandi remoti.

NOTA: l'indirizzo di posta elettronica NON deve essere un dominio locale. Si consiglia di adoperare l'indirizzo "rcommands@mailessentials.com". Non è richiesta l'esistenza di una cassetta postale per l'indirizzo configurato, ma la parte relativa al dominio dell'indirizzo deve essere un vero indirizzo di posta elettronica che restituisce un risultato positivo in caso di ricerca di registro MX tramite DNS.

3. In via facoltativa, è possibile configurare alcune elementari opzioni di protezione per i comandi remoti.

- Indicare una password condivisa da includere nel messaggio di posta elettronica. Per maggiori informazioni, consultare la sezione Uso dei comandi remoti del presente manuale.
- Inoltre, è possibile specificare quali utenti possono inviare messaggi di posta elettronica con comandi remoti.

NOTA: si noti che un utente potrebbe utilizzare tale opzione falsificando l'indirizzo di provenienza *From* (Da).

Le password sono inviate come comandi separati aventi la seguente sintassi:

PASSWORD: <shared password>;

5.7.2 Uso dei comandi remoti

I comandi remoti devono avere la seguente sintassi:

<command> : <param1>, [<param2>, <param3>, …];

Nel corpo di un messaggio di posta elettronica si possono inserire più comandi, ciascuno separato da un punto e virgola (;). Il nome di ogni comando deve essere riportato in LETTERE MAIUSCOLE perché distingue fra maiuscole e minuscole. Sono disponibili i seguenti comandi:

NOTA: il sistema può solo aggiungere parole chiavi, ma non modificarle o eliminarle. Non sono supportate condizioni.

I comandi disponibili sono:

- **ADDSUBJECT** - aggiunge parole chiave specifiche al data base del controllo parole chiave dell'oggetto.
  - **Esempio:** ADDSUBJECT: sesso, porno, spam;
- **ADDBODY** - aggiunge parole chiave specifiche al data base del controllo parole chiave del testo del messaggio di posta elettronica.
  - **Esempio:** ADDBODY: gratuito, "100% gratuito", "assolutamente gratuito";

NOTA: quando si deve specificare una frase anziché una singola parola, riportare la frase tra virgolette (" ")

5.7.3 Comandi di black list

Con i comandi di black list è possibile aggiungere alla black list

personalizzata un singolo indirizzo di posta elettronica o un intero dominio.

I comandi disponibili sono:

- **ADDBLIST:** <e-mail>;
  - **Esempio:** ADDBLIST: user@somewhere.com;

NOTA 1: per aggiungere un intero dominio alla black list, si deve specificare un carattere jolly prima del nome del dominio.

- **Esempio: ADDBLIST: *@domain.com.**

NOTA 2: per motivi di sicurezza, un messaggio di posta elettronica può contenere un solo comando ADDBLIST e si può indicare un singolo indirizzo come parametro di comando. Il parametro è l'indirizzo di posta elettronica di un utente o un dominio.

- **Esempio: spammer@spam.com o *@spammers.org.**

NOTA 3: si noti che nel nome di un dominio non sono consentiti caratteri jolly.

- **Esempio: *@*.domain.com viene respinta come non valida.**

5.7.4 Comandi per il filtro bayesiano

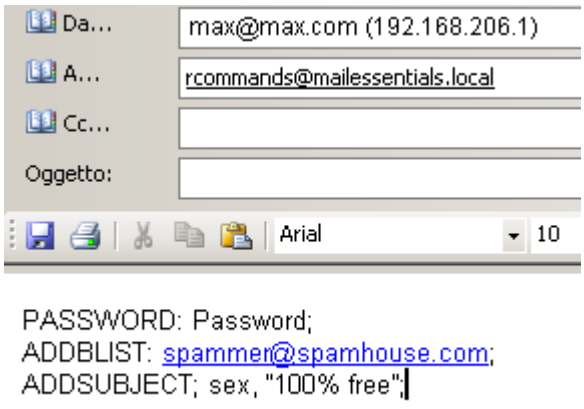
Con questi comandi è possibile aggiungere spam o ham (posta elettronica valida) al data base del filtro bayesiano. I comandi disponibili sono:

- **ADDASSPAM** - dà istruzione al filtro bayesiano di classificare quel dato messaggio di posta elettronica come spam.
- **ADDASGOODMAIL** - dà istruzione al filtro bayesiano di classificare quel dato messaggio di posta elettronica come ham.

NOTA: questi comandi non hanno parametri. Il parametro è costituito dalla parte restante del messaggio di posta elettronica.

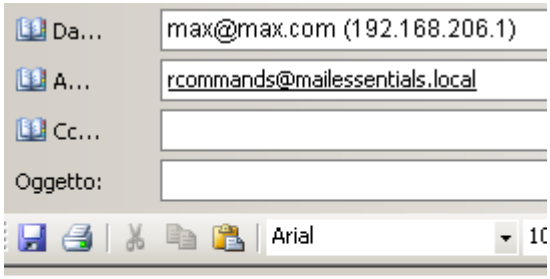
Esempi

- **Esempio 1** - Con l'invio di questo messaggio di posta elettronica l'utente aggiunge l'indirizzo spammer@spamhouse.com alla black list e, inoltre, aggiunge alcune parole chiave al data base del controllo parola chiave dell'oggetto.



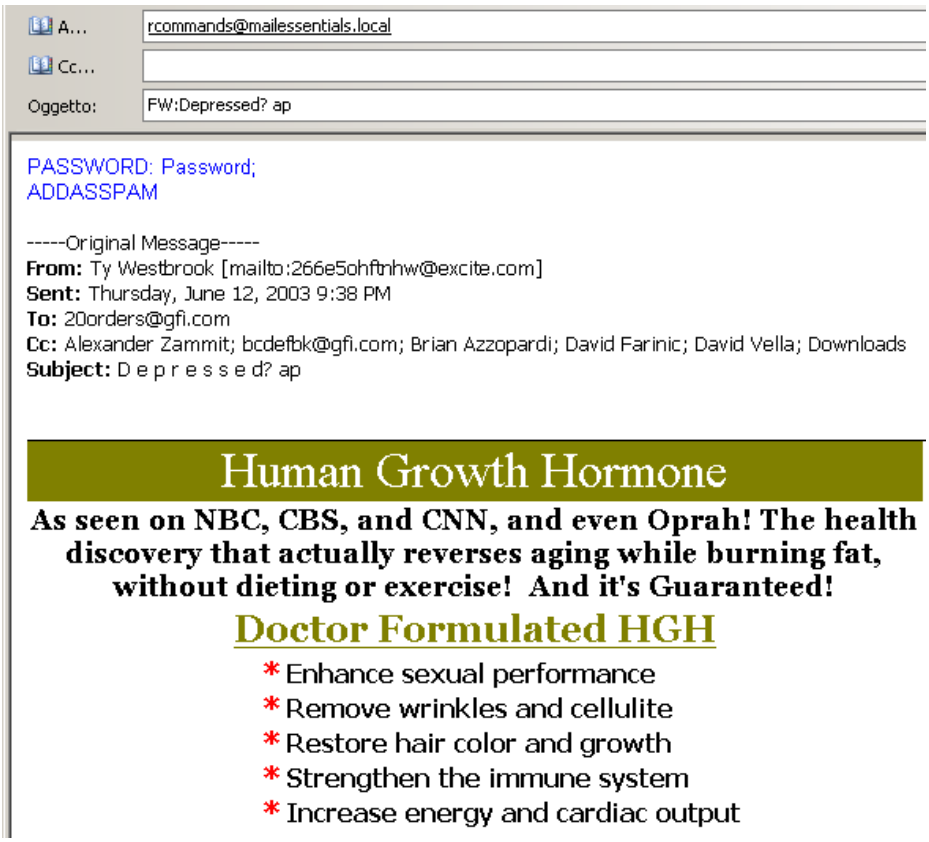
Schermata 88 - Aggiunta di indirizzi di posta elettronica alla black list e parole chiave

- Esempio 2 - È possibile indicare lo stesso comando più volte (in questo caso ADDBODY). Il risultato è cumulativo, cioè, in questo caso, le parole chiave aggiunte al data base di controllo del corpo del messaggio di posta elettronica sono: sesso, 100% gratuito e soldi subito.



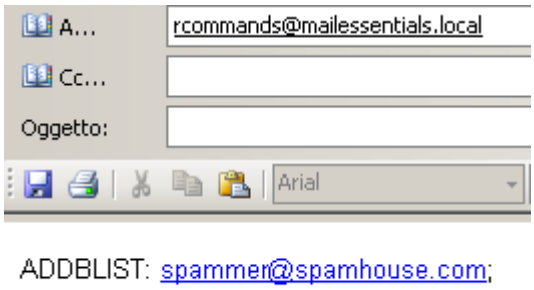
Schermata 89 - Indicazione degli stessi comandi più volte

- **Esempio 3:** Viene aggiunto un messaggio di spam tramite il comando ADDASSPAM. Si noti che per questo tipo di comando non sono richiesti i due punti (‘**:**’). Tutto quello che segue immediatamente il comando è trattato come dato dal filtro bayesiano.



Schermata 90 - Aggiunta di spam al data base del filtro bayesiano

- Esempio 4 - Quando risulta deselezionata la casella di controllo **Password condivisa** si possono inviare comandi remoti senza specificare una password.



Schermata 91 - Invio di comandi remoti senza protezione

5.7.5 Registrazione dei comandi remoti

Per conservare una traccia delle modifiche apportate, tramite i comandi remoti, al data base di configurazione, ogni messaggio di posta elettronica contenente comandi remoti (anche se non valida) viene salvato nella sottocartella "ADBRProcessed", situata nella cartella di root di GFI MailEssentials. Il nome del file di ciascun messaggio di posta elettronica è formattato secondo il seguente formato:

- **<sender_email_address>_SUCCESS_<timestamp>.eml** - in caso di elaborazione riuscita.
- **<sender_email_address>_FAILED_<timestamp>.eml** - in caso di elaborazione non riuscita.

NOTA: il formato temporale è aaaaggmmhhmmss.

5.8 Spostamento dei messaggi di spam nelle cartelle della cassetta postale dell'utente

Se su Microsoft Exchange Server è installato GFI MailEssentials, i messaggi di spam possono essere salvati in una cartella della cassetta postale dell'utente come descritto nel capitolo Azioni antispam: cosa fare dei messaggi di spam a pagina 73 di questo manuale.

Se su Microsoft Exchange Server NON è installato GFI MailEssentials, i messaggi di spam non possono essere indirizzati a una cartella specifica della cassetta postale dell'utente dalle Azioni antispam. Sarà, comunque, possibile indirizzare i messaggi di posta elettronica alla cassetta postale dell'utente come descritto qui di seguito.

5.8.1 Microsoft Exchange Server 2000/2003

GFI MailEssentials comprende un programma di utilità per la gestione delle regole, Rules Manager, che sposta automaticamente i messaggi etichettati come spam alla cassetta postale degli utenti.

NOTA: Rules Manager funziona solo su Windows 2000 e versioni successive.

IMPORTANTE: Per usare Rules Manager, selezionare l'opzione **Etichetta il messaggio con un testo specifico** nelle Azioni antispam e specificare un'etichetta.

Installare Rules Manager su Microsoft Exchange Server

1. Dal computer su cui è installato GFI MailEssentials andare alla cartella di installazione di GFI MailEssentials.

2. Copiare i file seguenti in una cartella su Microsoft Exchange Server:

- rulemgmtres.dll
- rulemgmt.exe
- rule.dll
- gfi_log.dll

3. Da Microsoft Exchange Server aprire la finestra di commando e spostare la directory nella posizione dove sono stati copiati i file Rules Manager.

4. Nella finestra di comando digitare: **regsvr32 rule.dll**

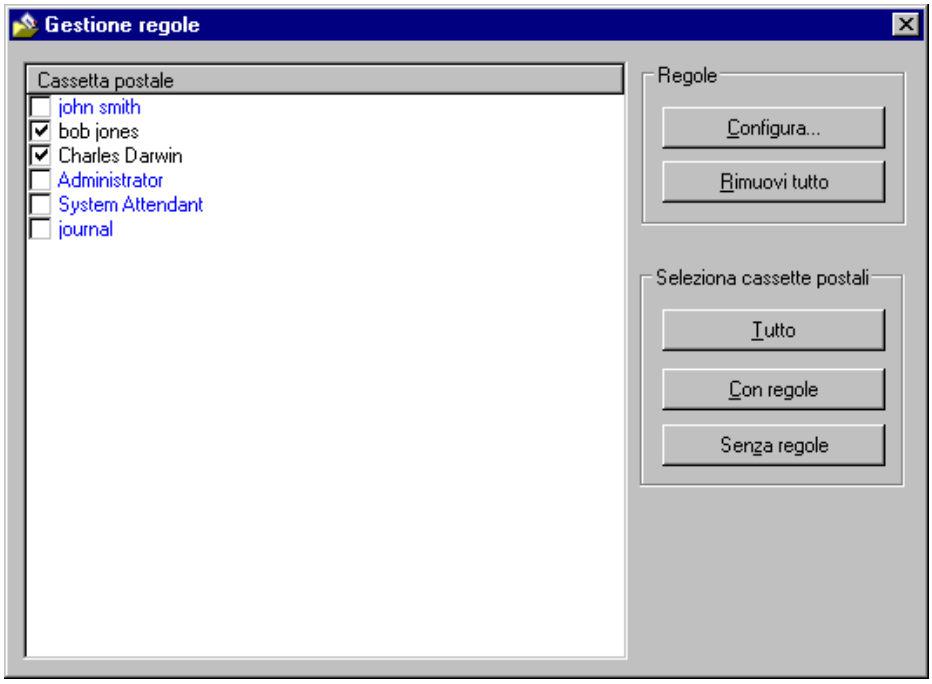
5. Fare clic su **OK** per confermare.

Avviare Rules Manager

1. Da Microsoft Exchange Server andare dove sono stati copiati i file Rules Manager e aprire **rulemgmt.exe**.

2. Selezionare un profilo Microsoft Outlook (profilo MAPI) o creare un nuovo profilo per l'accesso (solo quando si usa Rules Manager per la prima volta).

3. Fare clic su **OK** per avviare Rules Manager.



Schermata 10 - GFI MailEssentials Rules Manager

4. La finestra principale di Rules Manager mostra tutte le cassette postali abilitate su Microsoft Exchange Server. Il colore delle cassette postali indica lo stato della cassetta in questione:

- Blu - la cassetta postale ha delle regole configurate
- Nero - la cassetta postale non ha regole configurate.

Impostazione di nuove regole

1. Selezionare le cassette postali alle quali abbinare una regola e fare clic su **Configura…** per avviare la finestra di dialogo **Configura regola globale**.

NOTA 1: Alle cassette postali che contengono già delle regole è possibile aggiungere nuove regole.

NOTA 2: Selezionare più cassette postali per configurare l'applicabilità della stessa regola a tutte le cassette.

Schermata 11 - Aggiungere una nuova regola in Rules Manager

2. Nella casella di testo **Condizione regola** digitare l'etichetta data al messaggio di spam nelle azioni antispam di GFI MailEssentials.

3. Specificare l'**Azione regola**:

- selezionare **Elimina** per eliminare un messaggio di posta elettronica con un oggetto contenente una condizione regola
- selezionare **Sposta a:** per spostare un messaggio di spam in una cartella nella cassetta postale. Inserire il percorso della cartella dove salvare il messaggio di spam. Se si specifica **Posta in arrivo\Spam** si crea una cartella di spam nella cartella di Posta in arrivo. Se si specifica solo **Spam** la cartella viene creata nel livello superiore (lo stesso di quello della Posta in arrivo).

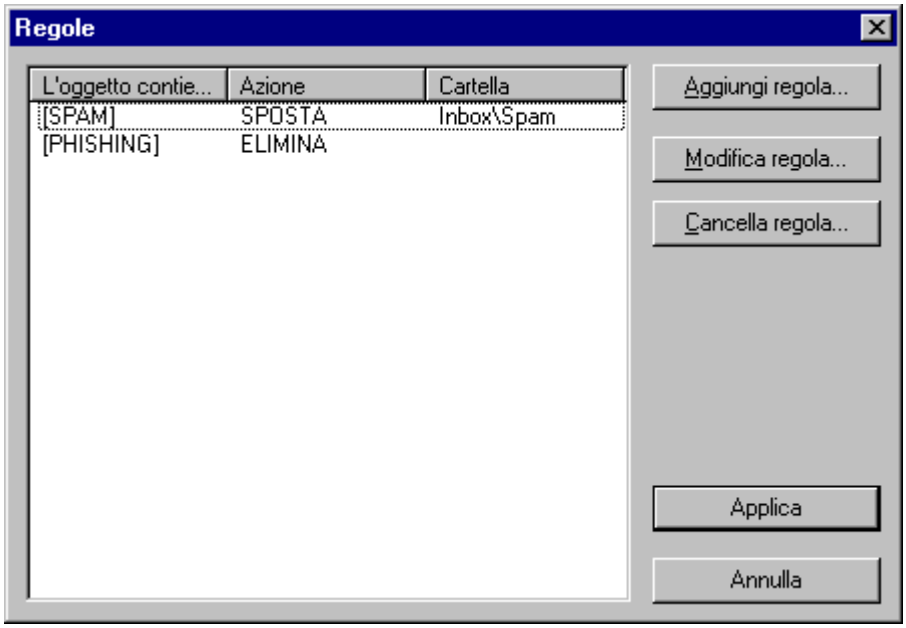
4. Fare clic su **Applica** per salvare le regole impostate.

Gestione di più regole

È possibile impostare più di una regola nella stessa cassetta postale.

Esempio: Eliminare i messaggi di posta elettronica etichettati come [Phishing] e spostare i messaggi etichettati come [SPAM] nella cartella Posta in arrivo\Spam.

1. Fare doppio clic su una cassetta postale per avviare la finestra di dialogo Regole.



Schermata 12 - Lista di regole in Rules Manager

2. Viene visualizzata una lista di regole applicabili alla casella di posta in arrivo selezionata.

- Fare clic su **Aggiungi regola** per aggiungere una nuova regola
- Selezionare una regola e fare clic su **Modifica regola** per cambiare le impostazioni della regola selezionata
- Selezionare una regola e fare clic su **Elimina regola** per eliminare la regola selezionata.

3. Fare clic su **Applica** per salvare le impostazioni.

5.8.2 Microsoft Exchange 2007/2010

Per configurare Microsoft Exchange 2007/2010 per inoltrare i messaggi etichettati verso la cartella di posta indesiderata dell'utente è necessario creare una Regola di trasporto.

IMPORTANTE: Selezionare solo l'opzione **Etichetta il messaggio con un testo specifico** nelle Azioni antispam di GFI MailEssentials.

Se si seleziona un'altra azione i messaggi di posta elettronica individuati come spam non arriveranno alla cassetta postale dell'utente e, quindi, le regole di trasporto configurate non saranno applicabili.

Per creare una Regola di trasporto in Exchange 2007/2010:

1. Avviare la **Console di gestione di Microsoft Exchange**.

2 Andare su **Microsoft Exchange ► Configurazione organizzazione ► Trasporto Hub** e selezionare il nodo **Regole di trasporto**.

3. Fare clic su **Nuova regola di trasporto** per eseguire la procedura guidata.

4. Digitare un nome per la nuova regola (ad esempio SPAM GFI MailEssentials) e fare clic su **Avanti**.

5. Nell'area **Condizioni** selezionare l'opzione **Quando il campo dell'oggetto contiene parole specifiche**.

6. Nell'area **Modifica regola** fare clic su **Parole specifiche** per inserire le parole da usare per l'etichettatura. Digitare l'etichetta specificata nelle Azioni antispam di ogni filtro antispam e fare clic su **Aggiungi** (ad esempio [SPAM]). Una volta aggiunte tutte le parole fare clic su **OK** e quindi su **Avanti**.

7. Nell'area Azioni selezionare l'opzione **Imposta il livello di confidenza dello spam su un valore**.

8. Nell'area **Modifica regola** fare clic su **0** e impostare il livello di confidenza su **9**. Fare clic su **OK** e quindi su **Avanti**.

9. (Facoltativo) Impostare eventuali eccezioni per questa regola di trasporto e fare clic su **Avanti**.

10. Fare clic su **Nuova** per creare la nuova Regola di trasporto.

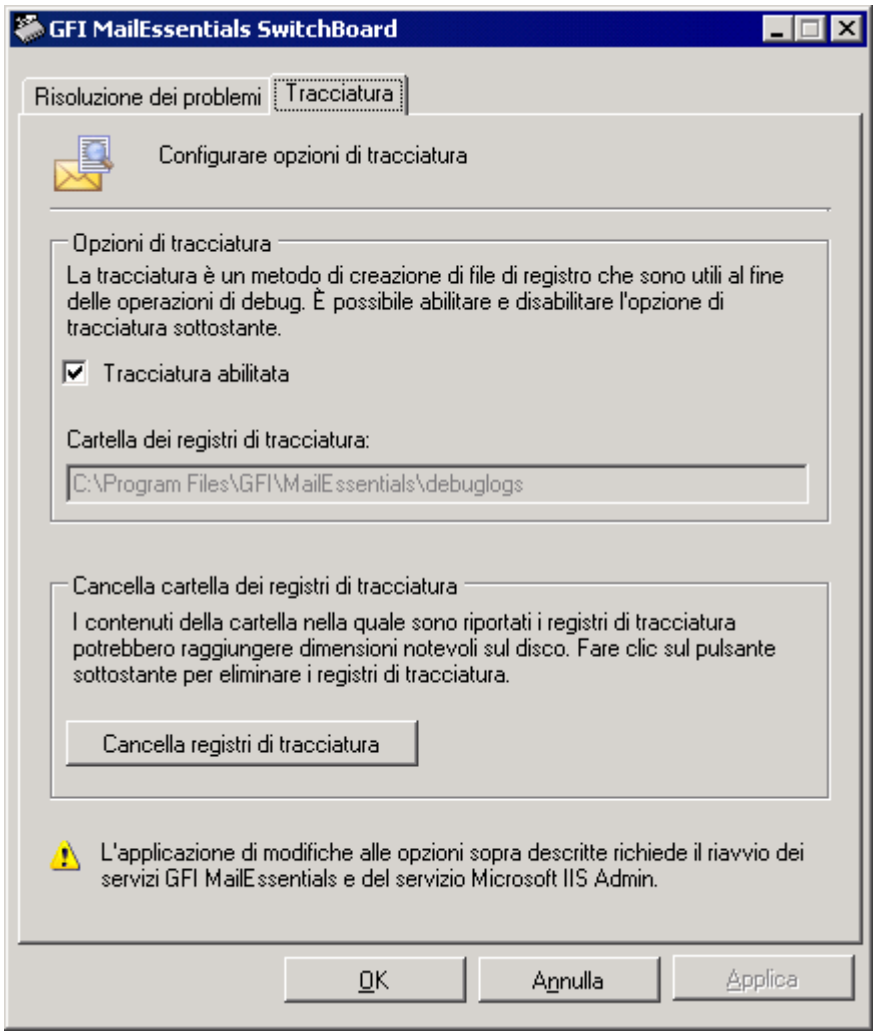
NOTA: Assicurarsi che la cartella di Posta indesiderata sia abilitata per le cassette postali degli utenti.

A questo punto la regola di trasporto creata inoltrerà tutti i messaggi di posta elettronica contenenti l'etichetta GFI MailEssentials alla cartella di posta indesiderata degli utenti.

5.9 Tracciatura

GFI MailEssentials è in grado di creare registri ai fini della risoluzione dei problemi. Quando è abilitato, GFI MailEssentials archivia i registri nella cartella DebugLogs all'interno della cartella di installazione di GFI MailEssentials. Per configurare la Tracciatura:

1. Andare su **Start ► Programmi ► GFI MailEssentials ► GFI MailEssentials Switchboard**.



Schermata 13 - Tracciatura

2. Selezionare la scheda **Tracciatura** e configurare le opzioni seguenti:

- Per abilitare/disabilitare la tracciatura selezionare/deselezionare la casella di controllo **Tracciatura abilitata**. Questa opzione è abilitata per impostazione predefinita.
- Fare clic su **Cancella registri di tracciatura** per eliminare tutti i registri

Backup dei messaggi di posta prima/dopo l'elaborazione

IMPORTANTE: Si consiglia vivamente di lasciare questa opzione deselezionata e usarla solo ai fini della risoluzione dei problemi, sotto la raccomandazione di personale professionista.

Dalla scheda **Risoluzione dei problemi**, selezionare/deselezionare la casella di controllo **Conservare una copia di ogni messaggio di posta elettronica prima e dopo l'elaborazione dei messaggi** per archiviare una copia di ogni messaggio di posta elettronica elaborato nella cartella SinkArchives all'interno della cartella di installazione di GFI MailEssentials.

6 Risoluzione dei problemi e assistenza

6.1 Introduzione

Questo capitolo descrive le modalità per risolvere eventuali problemi riscontrati durante l'installazione di GFI MailEssentials. Le principali fonti di informazioni disponibili per gli utenti sono le seguenti:

1. il presente manuale
2. le seguenti sezioni riguardanti le questioni comuni
2. gli articoli di GFI Knowledge Base
3. i controlli consueti
4. i forum via Web
5. contattando l'assistenza tecnica di GFI

6.2 Manuale dell'utente

Le informazioni contenute nel presente manuale dell'utente consentono di capire la causa dei problemi durante l'installazione di GFI MailEssentials. Le sezioni informative unitamente alle sezioni riguardanti i problemi comuni qui di seguito offrono orientamenti sulle azioni da svolgere per risolvere problemi che potrebbero essere dovuti a una errata configurazione o a errore umano.

6.3 Problemi comuni

I problemi comuni di seguito elencati consentiranno di verificare i problemi comuni riscontrati dagli utenti durante l'utilizzo di GFI MailEssentials.

6.3.1 Gestione dello spam

Problema riscontrato	Soluzione
1. La dashboard indica che non vengono elaborati messaggi di posta elettronica; o vengono elaborati solamente i messaggi in arrivo o in uscita	1. Accertarsi che GFI MailEssentials non sia disabilitato a eseguire la scansione dei messaggi. Per maggiori informazioni, consultare la sezione Abilitazione/Disabilitazione della scansione dei messaggi di posta elettronica del presente manuale. 2. Verificare i server virtuali multipli SMTP IIS Microsoft e accertarsi che GFI MailEssentials sia collegato al server virtuale corretto. 3. Il record MX del dominio non è configurato correttamente. Accertarsi che il record MX indichi l'indirizzo IP del server di GFI MailEssentials 4. Se i messaggi in arrivo passano attraverso un altro gateway, accertarsi che il server di posta sull'altro gateway inoltri i messaggi in arrivo attraverso GFI MailEssentials 5. Accertarsi che i messaggi in uscita siano configurati per essere

	indirizzati attraverso GFI MailEssentials. Consultare il manuale di installazione per maggiori dettagli. 6. Verificare che il server virtuale SMTP usato da Microsoft Exchange Server per i messaggi in uscita sia lo stesso server SMTP a cui GFI MailEssentials è collegato. Per maggiori informazioni sulla modalità di risoluzione di questo problema, consultare: http://kbase.gfi.com/showarticle.asp?id=KBID003286
2. Dopo aver installato GFI MailEssentials, alcuni messaggi mostrano un corpo del messaggio confuso se visualizzato in Microsoft Outlook o GFI MailArchiver	Questo problema si verifica per i messaggi che adoperano una serie di caratteri per l'intestazione del messaggio e un carattere diverso per il corpo del messaggio. Quando vengono elaborati da Microsoft Exchange 2003, questi messaggi si presenteranno confusi con Microsoft Outlook e GFI MailArchiver. Microsoft ha realizzato un *hotfix* per risolvere questo problema. Per maggiori informazioni sulla modalità di risoluzione di questo problema, consultare: http://kbase.gfi.com/showarticle.asp?id=KBID003459 e http://support.microsoft.com/kb/916299

6.3.2 Archiviazione e rapporti

Problema riscontrato	Soluzione
1. I messaggi etichettati come spam vengono archiviati	1. Eseguire Rules Manager sul computer Microsoft Exchange facendo doppio clic su "rulemgmt.exe" dalla cartella di GFI MailEssentials. 2. Abilitare la casella di controllo accanto al nome della cassetta postale sottoposta a polling da parte di GFI MailArchiver ai fini dell'archiviazione. 3. Fare clic su **Configura** e accertarsi che le impostazioni "Condizione regola" e "Azione regola" siano corrette. Fare clic su **Applica**. Per maggiori informazioni sulla modalità di risoluzione di questo problema, consultare: http://kbase.gfi.com/showarticle.asp?id=KBID002747
2. Non è possibile accedere ad AWI secondo il messaggio "HTTP Error 404 - File o directory not found"	Per impostazione predefinita, "Internet Information Services (IIS)" disabilita il contenuto dinamico. AWI richiede la sua attivazione, dal momento che i dati vengono recuperati in modo dinamico dal data base dell'archivio. 1. Caricare IIS Manager, espandere il nodo ***<Server Name>*** ►le estensioni **Web service** e fare clic con il pulsante destro del mouse su "Active Server Pages". 2. Fare clic su Consenti per impostare lo stato su "consentito". Per maggiori informazioni sulla modalità di risoluzione di questo problema, consultare: http://kbase.gfi.com/showarticle.asp?id=KBID002963
3. I dati precedenti non sono disponibili nel data base se si utilizza Microsoft Access.	Quando il data base reports.mdb supera 1.7Gb, il data base viene automaticamente rinominato come *reports_<data>.mdb* e viene creato un nuovo rapporto reports.mdb. Per maggiori informazioni sulla modalità di risoluzione di questo problema, consultare: http://kbase.gfi.com/showarticle.asp?id=KBID003422

6.3.3 Azioni e filtri antispam

Problema riscontrato	Soluzione
1. Lo SPAM arriva nella cassetta	Seguire l'elenco di controllo in basso per risolvere questo

postale degli utenti	problema. 1. Accertarsi che la scansione dei messaggi di GFI MailEssentials non sia disabilitata. Per maggiori informazioni sulla modalità di avvio della scansione, consultare la sezione Abilitazione/Disabilitazione della scansione dei messaggi di posta elettronica del presente manuale. 2. Verificare che tutti i filtri antispam richiesti siano abilitati 3. Verificare se i domini locali siano configurati correttamente 4. Verificare se i messaggi di posta passano attraverso GFI MailEssentials o se GFI MailEssentials è collegato al server virtuale SMTP IIS 5. Verificare se la posizione "%TEMP%" (che per impostazione predefinita è la cartella "C:\Windows\Temp" contiene molti file 6. Verificare se il numero di utenti che usa GFI MailEssentials supera il numero di licenze acquistate 7. Verificare che la white list sia configurata correttamente 8. Verificare che le azioni siano configurate correttamente 9. Verificare che il filtro bayesiano sia configurato correttamente Per maggiori informazioni sulla modalità di risoluzione di questo problema, consultare: http://kbase.gfi.com/showarticle.asp?id=KBID003256
2. Le black list personalizzate e/o le pagine del controllo parole chiave impiegano troppo tempo per caricarsi o sembrano bloccate	Limitare il numero di voci a 10.000 negli elenchi di GFI MailEssentials. Per maggiori informazioni sulla modalità di risoluzione di questo problema, consultare: http://kbase.gfi.com/showarticle.asp?id=KBID002915 e: http://kbase.gfi.com/showarticle.asp?id=KBID003267
3. Gli aggiornamenti di SpamRazer non vengono scaricati	1. Accertarsi di avere una chiave di licenza valida. 2. Accertarsi che le porte necessarie siano aperte e che il firewall sia configurato in modo tale da consentire le connessioni dal server di GFI MailEssentials a qualsiasi server proxy, secondo la propria configurazione. Per maggiori informazioni sulla modalità di risoluzione di questo problema, consultare: http://kbase.gfi.com/showarticle.asp?id=KBID002184

6.3.4 Declinazione di responsabilità

Problema riscontrato	Soluzione
1. Le declinazioni di responsabilità non sono aggiunte ai messaggi di posta elettronica in uscita.	Verificare se i domini locali siano configurati correttamente. Consultare la Guida introduttiva per maggiori informazioni.
2. Alcuni caratteri nel testo della declinazione di responsabilità non vengono visualizzati correttamente.	Configurare Microsoft Outlook in modo tale che non proceda alla codificazione automatica e costringere un oggetto Criteri di gruppo a utilizzare la codificazione corretta. Per maggiori informazioni sulla modalità di risoluzione di questo problema, consultare: http://office.microsoft.com/en-us/ork2003/HA011402641033.aspx
3. La declinazione di responsabilità viene inviata anche se questa opzione è disabilitata.	Affinché le modifiche abbiano effetto, riavviare i servizi IIS e GFI MailEssentials dopo aver disabilitato una declinazione di responsabilità.

6.3.5 Monitoraggio dei messaggi di posta elettronica

Problema riscontrato	Soluzione

1. I messaggi ricevuti o inviati da certi utenti non vengono monitorati.	Le regole di monitoraggio dei messaggi di posta elettronica non monitorano i messaggi inviati o ricevuti dall'amministratore di GFI MailEssentials e l'indirizzo di posta elettronica a cui i messaggi monitorati vengono inviati. Le regole di monitoraggio dei messaggi di posta elettronica non sono inoltre disponibili per i messaggi inviati tra utenti interni previsti nel medesimo archivio informativo.

6.3.6 Server di elenco

Problema riscontrato	Soluzione
1. I messaggi inviati al server di elenco si convertono in testo.	I messaggi inviati al server di elenco vengono convertiti in messaggi di testo solamente quando il formato originale del messaggio è RTF. Inviare il messaggio in formato HTML per conservare il formato originale.
2. Gli utenti interni ricevono un rapporto di mancato recapito quando inviano un messaggio al server di elenco, se GFI MailEssentials è installato su un computer gateway.	Per maggiori informazioni sulla modalità di utilizzo della funzionalità del server di elenco se GFI MailEssentials è installato su un gateway, consultare: http://kbase.gfi.com/showarticle.asp?id=KBID002123

6.3.7 Funzioni varie

Problema riscontrato	Soluzione
1. La dashboard riferisce il seguente errore: "Utente o password errati nel tentativo di connettersi al server POP3…"	Accertarsi che il servizio dell'archivio informative Microsoft Exchange Information sia avviato. Per maggiori informazioni sulla modalità di risoluzione di questo problema, consultare: http://kbase.gfi.com/showarticle.asp?id=KBID001805
2. I clienti connessi a Microsoft Exchange mediante "POP3" non sono in grado di visualizzare i messaggi bloccati come SPAM.	Connettersi a Microsoft Exchange usando IMAP. Per maggiori informazioni sulla modalità di risoluzione di questo problema, consultare: http://kbase.gfi.com/showarticle.asp?id=KBID002644
3. Gli aggiornamenti automatici non riescono mentre lo scaricamento di quelli manuali mediante GFI MailEssentials configuration funziona.	Verificare che le connessioni non autenticate siano consentite dal computer su cui è installato GFI MailEssentials a http://update.gfi.com, porta 80. Per maggiori informazioni sulla modalità di risoluzione di questo problema, consultare: http://kbase.gfi.com/showarticle.asp?id=KBID002116
4. I dati di configurazione non possono essere importati.	Accertarsi che la versione e la build di GFI MailEssentials siano identiche nelle installazioni sorgente e di destinazione. Per maggiori informazioni sulla modalità di risoluzione di questo problema, consultare: http://kbase.gfi.com/showarticle.asp?id=KBID003182
5. I comandi remoti non funzionano.	Per informazioni sulla modalità di risoluzione di questo problema, consultare: http://kbase.gfi.com/showarticle.asp?id=KBID001806

6.4 Knowledge Base

GFI cura la gestione di una Knowledge Base completa contenente le risposte ai problemi più comuni.

Se le informazioni contenute in questo manuale non aiutano a risolvere i problemi di installazione, fare riferimento alla Knowledge Base. La Knowledge Base riporta sempre le domande di assistenza tecnica e le patch più aggiornate. La Knowledge Base è disponibile

alla pagina:

http://kbase.gfi.com/

6.5 Controlli consueti

Se le informazioni contenute in questo manuale e la Knowledge Base non aiutano a risolvere i problemi:

1. verificare che tutti i pacchetti di servizi del sistema operativo, il server di posta e GFI MailEssentials siano installati.

2. Installare nuovamente Microsoft Data Access Components (MDAC) per assicurarne il corretto funzionamento.

6.6 Forum via Web

L'assistenza tecnica tra utenti è disponibile sul forum via Web di GFI. Dopo aver fatto riferimento alle informazioni nel manuale dell'utente e nella Knowledge Base, accedere al forum via Web visitando:

http://forums.gfi.com/.

6.7 Richiesta di assistenza tecnica

Se nessuna delle risorse summenzionate ha contribuito a risolvere i problemi, contattare il personale di assistenza tecnica compilando il modulo di richiesta online o telefonando.

- **Online:** compilare il modulo di richiesta di assistenza e seguire attentamente le istruzioni di questa pagina per inviare la richiesta di assistenza a: http://support.gfi.com/supportrequestform.asp.
- **Telefono:** per ottenere il numero telefonico corretto dell'assistenza tecnica della regione competente, visitare: http://www.gfi.com/company/contact.htm.

NOTA: prima di contattare l'assistenza tecnica di GFI, accertarsi di avere a disposizione l'ID cliente. L'ID cliente è il numero dell'account cliente online assegnato alla prima registrazione delle chiavi di licenza nell'Area clienti su:

http://customers.gfi.com.

GFI tenta di rispondere alle richieste entro 24 ore, in funzione dell'ora locale dell'utente.

6.8 Notifiche relative alle build

Si consiglia fortemente di iscriversi al nostro elenco di notifiche relative alle build. In questo modo si viene immediatamente informati sulle nuove build del prodotto. Per iscriversi a tale servizio, visitare il sito:

http://www.gfi.com/pages/productmailing.htm

6.9 Documentazione

Se questo manuale non soddisfa le attese o si ritiene che possa in qualche modo essere migliorato, scrivere un messaggio di posta elettronica a: documentation@gfi.com

7 Appendice 1 - Modalità di funzionamento del filtraggio antispam

7.1 Filtraggio della posta in arrivo

Il filtraggio della posta in arrivo è il processo attraverso il quale i messaggi di posta elettronica in entrata vengono filtrati prima di essere consegnati agli utenti.

1. Nello stabilire una connessione, viene controllato l'indirizzo di posta elettronica del destinatario del messaggio in entrata. Qualora non venisse trovato, la connessione viene terminata immediatamente. Tale operazione viene eseguita attraverso il filtro di raccolta di directory Se l'indirizzo di posta elettronica del destinatario viene trovato, il messaggio di posta elettronica passa alla fase successiva.

2. Il messaggio di posta elettronica viene analizzato per vedere se è inoltrato ad un server nell'elenco remoto, In tal caso viene inoltrato, altrimenti passa alla fase successiva.

3. Il messaggio di posta elettronica in entrata viene filtrato da tutti i filtri antispam. Tutti i messaggi di posta elettronica che non superano la verifica di un filtro antispam vengono inviati alle azioni antispam di posta elettronica. Se un messaggio di posta elettronica supera la verifica di tutti i filtri e non viene identificato come spam, passa alla fase successiva.

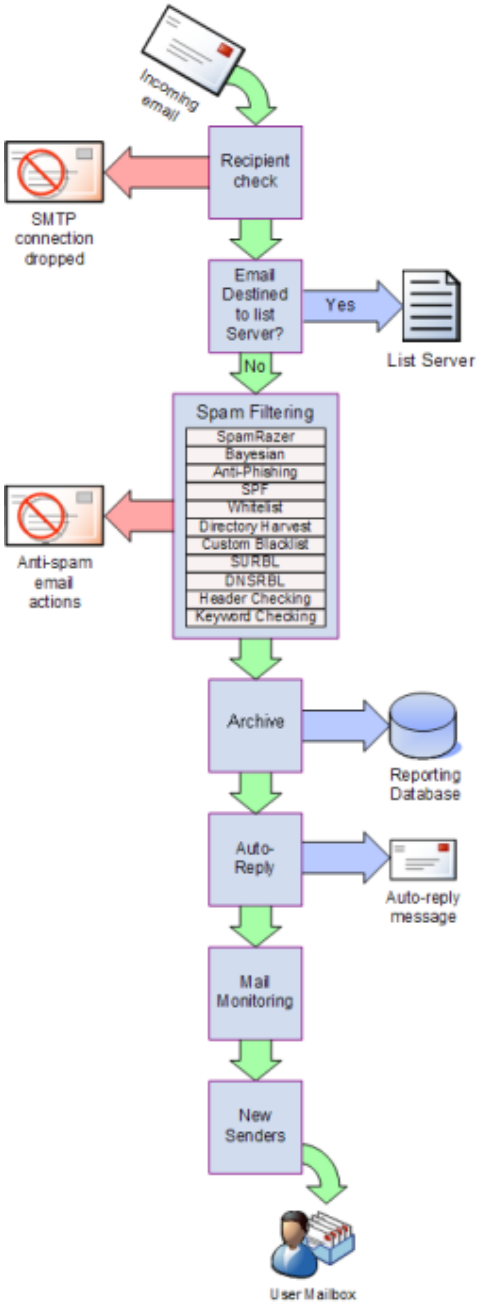
4. Il messaggio di posta elettronica viene archiviato nel data base di riferimento, se questa opzione è configurata. Il messaggio passa alla fase successiva.

5. Le risposte automatiche vengono quindi inviate al mittente, se questa opzione è configurata. Il messaggio passa alla fase successiva.

6. Il monitoraggio della posta elettronica viene successivamente eseguito e vengono prese le misure opportune, se questa opzione è configurata. Il messaggio passa alla fase successiva.

7. Il filtro Nuovi Mittenti viene a questo punto attivato. Il messaggio passa alla fase successiva.

8. Il messaggio di posta elettronica viene inviato alla cassetta postale dell'utente.



7.1.1 Domini di posta elettronica in arrivo

GFI MailEssentials conferisce molta importanza al concetto dei domini di posta elettronica in arrivo. Durante la configurazione, GFI MailEssentials rileverà automaticamente i domini su cui ricevere i messaggi di posta elettronica, consentendo di fare la distinzione tra messaggi in arrivo e messaggi in uscita e proteggere in questo modo la rete da spam. I domini di posta elettronica in arrivo sono inoltre configurabili dopo l'installazione attraverso la console di GFI MailEssentials configuration. Per maggiori informazioni, consultare la guida "Amministrazione e configurazione" di GFI MailEssentials.

7.2 Filtraggio della posta in uscita

Il filtraggio della posta in uscita è il processo attraverso il quale la posta elettronica inviata dagli utenti all'interno di un'azienda viene elaborata prima di essere inviata.

1. L'utente crea e invia messaggi di posta elettronica.

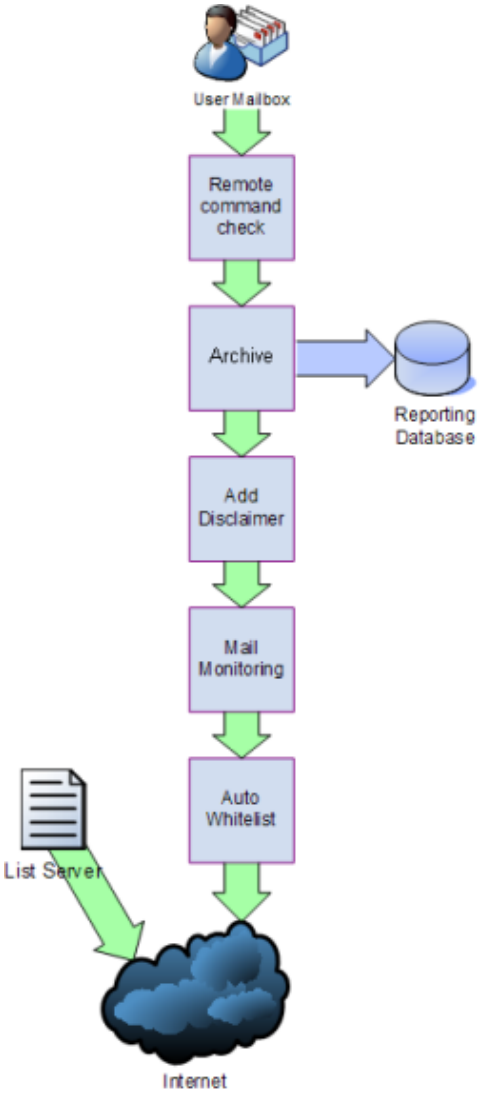
2. La funzione comandi remoti controlla gli eventuali comandi attivati dai messaggi. Se non ne sono presenti, il messaggio passa alla fase successiva

3. Il messaggio di posta elettronica viene poi controllato per valutare se debba essere archiviato. Se la funzione di archiviazione è abilitata, il messaggio di posta elettronica viene salvato nel data base di riferimento. In tutti i casi, il messaggio passa alla fase successiva.

4. Se configurata, la declinazione di responsabilità applicabile viene aggiunta poi al messaggio. Quindi il messaggio passa alla fase successiva.

5. Il messaggio di posta elettronica viene sottoposto a controllo ai fini del monitoraggio applicabile e viene eseguita l'azione secondo le regole configurate. Il messaggio passa alla fase successiva.

6. Se l'opzione è abilitata, il controllo automatico della white list aggiunge l'indirizzo di posta elettronica del destinatario del messaggio alla white list. Ciò consente alle risposte di tali destinatari di essere inviate in via automatica al mittente, senza verifica. Dopo questo controllo, i messaggi di posta elettronica vengono inviati ai destinatari.



La sequenza degli eventi della posta elettronica in uscita viene seguita da tutti i messaggi in uscita, tranne per i processi di posta elettronica in uscita avviati dal server di elenco.. Questa funzionalità consente la creazione e l'indirizzamento delle liste di distribuzione (newsletter e liste di discussione) da GFI MailEssentials. In questo caso i messaggi vengono sottoposti a scansione e inviati automaticamente ai destinatari.

8 Appendice 2 - Filtraggio bayesiano

Il filtro bayesiano costituisce la tecnologia di lotta allo spam di GFI MailEssentials. La tecnologia di filtraggio bayesiano è una tecnica adattiva, di algoritmi di "intelligenza artificiale", resi più rigorosi per far fronte alla più estesa serie di tecniche di spam disponibili oggi.

Il presente capitolo spiega il funzionamento del filtro bayesiano e le sue modalità di configurazione e addestramento.

NOTA: il filtro antispam bayesiano è disabilitato per impostazione predefinita. Si raccomanda vivamente di addestrare il filtro bayesiano prima di abilitarlo.

IMPORTANTE: GFI MailEssentials deve funzionare per almeno una settimana affinché il filtro bayesiano possa offrire una prestazione ottimale, perché il filtro bayesiano raggiunga la più alta percentuale d'individuazione dello spam adattandosi in maniera specifica ai modelli di posta elettronica dell'utente.

Modalità di funzionamento del filtro antispam bayesiano

Il filtraggio bayesiano si basa sul principio che la maggior parte degli eventi è interdipendente e la probabilità che un evento si verifichi in futuro può essere dedotta dal verificarsi di quello stesso evento in precedenza.

NOTA: ulteriori informazioni sulle basi matematiche del filtraggio bayesiano sono disponibili ai seguenti link:

http://www-ccrma.stanford.edu/~jos/bayes/Bayesian_Parameter_Estimation.html

http://www.niedermayer.ca/papers/bayesian/bayes.html

La stessa tecnica è usata da GFI MailEssentials per individuare e classificare lo spam. In presenza di parti di testo contenute spesso in messaggi di spam ma non in un messaggio di posta elettronica legittima, è ragionevole presumere che tali messaggi costituiscano probabilmente dello spam.

Creazione di un data base di parole specifico per il filtro bayesiano

Prima di poter filtrare i messaggi con questo metodo, l'utente deve generare un data base di termini e simboli (quali il simbolo $, gli indirizzi e domini IP, ecc.) raccolti da campioni di messaggi di spam e di messaggi validi (denominati "ham").

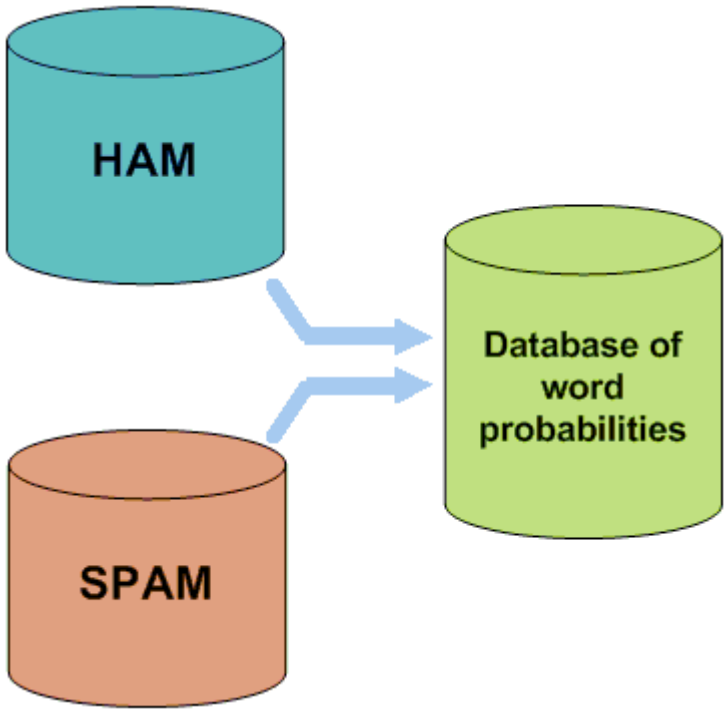


Figura 1 - Creazione di un data base di termini per il filtro

A ciascun termine o simbolo viene quindi assegnato un valore di probabilità. Tale valore è calcolato considerando la frequenza con cui un termine compare nello spam rispetto a quella di un messaggio legittimo “ham”. A tale scopo, si analizzano i messaggi di posta elettronica in uscita degli utenti e lo spam conosciuto: tutti i termini e i simboli in entrambi i pool di posta elettronica vengono analizzati per generare la probabilità che un termine specifico porti a rilevare un messaggio come spam.

La probabilità del termine si calcola come segue:

se il termine “ipoteca”, per esempio, è presente in 400 messaggi di spam su 3.000 e in 5 messaggi legittimi su 300, il valore di probabilità dello spam sarà pari a 0,8889 (cioè, [400/3000] diviso per [5/300+400/3000]).

Creazione di un data base ham personalizzato

È importante notare che l’analisi dei messaggi ham è eseguita sulla posta elettronica dell’azienda ed è pertanto configurata sulle esigenze di quella specifica azienda.

- **Esempio:** un istituto finanziario può utilizzare il termine “mutuo” abbastanza spesso e quindi, in questo caso, l’utilizzo di una serie di regole antispam generica potrebbe produrre molti falsi positivi. Del resto, il filtro bayesiano, se adattato all’azienda attraverso un periodo iniziale di addestramento, prende nota dei messaggi validi in uscita dell’azienda (cioè, riconosce che la parola “mutuo” è usata spesso in messaggi legittimi) e quindi offre una migliore percentuale di individuazione dello spam e una più bassa probabilità di incorrere in falsi positivi.

Creazione del data base antispam bayesiano

Oltre che ai messaggi ham, il filtro bayesiano si affida anche a un file

di dati spam. Questo file di dati spam deve contenere un ampio campione di spam noto e va costantemente aggiornato con lo spam più recente da parte del software antispam. In questo modo si assicura che il filtro bayesiano sia a conoscenza dei trucchi di spam più recenti, producendo un'elevata percentuale di individuazione dello spam.

Modalità di esecuzione effettive del filtraggio bayesiano

Una volta creati i data base ham e spam, è possibile calcolare i valori di probabilità dei termini e il filtro è quindi pronto per l'uso.

All'arrivo di un nuovo messaggio di posta elettronica, lo si scompone in parole e, tra queste ultime, si scelgono le più pertinenti, vale a dire, quelle più significative ai fini dell'identificazione o meno del messaggio di spam. Dall'analisi di tali parole, il filtro bayesiano calcola la probabilità che il nuovo messaggio possa essere o meno uno spam. Se il valore di probabilità è maggiore di un certo valore di soglia, il messaggio è classificato come spam.

NOTA: per maggiori informazioni sul filtraggio bayesiano e i suoi vantaggi, consultare:

http://kbase.gfi.com/showarticle.asp?id=KBID001813

9 Glossario

Active Directory	Una tecnologia che fornisce una varietà di servizi di rete, compresi i servizi di directory tipo LDAP.
AD	*Vedere* Active Directory
Azioni antispam	Azioni eseguite su messaggi di spam ricevuti, per es., eliminare un messaggio o inviarlo nella cartella di Posta indesiderata.
Background Intelligent Transfer Service	Una componente dei sistemi operativi di Microsoft Windows che agevola il trasferimento di file tra i sistemi, usando la banda di rete passiva.
BITS	*Vedere* Background Intelligent Transfer Service
Black list	Un elenco di utenti o domini di posta elettronica dai quali gli utenti non possono ricevere messaggi
Botnet	Software maligno che si attiva in modo autonomo e automatico controllato da un hacker/cracker.
Cartella pubblica	Una cartella comune che permette agli utenti di Microsoft Exchange di condividere informazioni.
Comandi remoti	Istruzioni che agevolano la possibilità di eseguire attività a distanza.
Declinazione di responsabilità	Una dichiarazione tesa a individuare o limitare l'ambito dei diritti e dei doveri per i destinatari dei messaggi di posta elettronica.
DMZ	*Vedere* Zona demilitarizzata
DNS	*Vedere* Domain Name System
DNS MX	*Vedere* Mail Exchange
Domain Name System	Un data base usato dalle reti TCP/IP per la traduzione di *hostname* in numeri IP e fornire altre informazioni riguardanti il dominio.
Falsi positivi	Un risultato errato che individua un messaggio come spam quando in realtà non lo è.
Filtraggio bayesiano	Una tecnica antispam dove un indice di probabilità statistica basata sulla formazione degli utenti viene usato per individuare lo spam.
Ham	Messaggio di posta elettronica legittimo
IIS	*Vedere* Internet Information Services
IMAP	*Vedere* Internet Message Access Protocol
Internet Information Services	Una serie di servizi basati su Internet creati da Microsoft Corporation per server di Internet.
Internet Message Access Protocol	Uno dei protocolli standard Internet più comunemente usati per il recupero di messaggi di posta elettronica, l'altro è POP3.
LDAP	*Vedere* Lightweight Directory Access Protocol

Lightweight Directory Access Protocol	Un protocollo di applicazione usato per interrogare e modificare i servizi di directory attivi su TCP/IP
Mail Exchange	Un registro usato da DNS per fornire nomi di altre entità a cui dovrebbe essere inviato un messaggio di posta elettronica.
MAPI	*Vedere* Messaging Application Programming Interface
MDAC	*Vedere* Microsoft Data Access Components
Messaging Application Programming Interface	Un'architettura di messaggistica e un Component Object Model basato su API per Microsoft Windows.
Microsoft Data Access Components	Una tecnologia Microsoft che offre agli sviluppatori un modo uniforme e coerente di sviluppare software che possono accedere a quasi tutti gli archivi di dati.
Microsoft Message Queuing Services	Un servizio accodamento messaggi per i sistemi operativi Windows Server.
MIME	*Vedere* Multipurpose Internet Mail Extensions
MSMQ	*Vedere* Microsoft Message Queuing Services
Multipurpose Internet Mail Extensions	Uno standard che estende il formato di un messaggio di posta elettronica per supportare il testo diverso da ASCII, allegati in formato non di testo, corpi del messaggio con parti multiple e informazioni collocate all'intestazione in serie di caratteri non ASCII.
NDR	*Vedere* Rapporto di mancato recapito
Phishing	Il processo di acquisire informazioni personali sensibili allo scopo di frodare le persone, in genere attraverso l'uso di comunicazioni fasulle.
POP2Exchange	Un sistema che raccoglie i messaggi di posta elettronica dalle cassette di posta POP3 e li indirizza al server di posta.
POP3	Vedere Post Office Protocol ver.3
Post Office Protocol ver.3	Un protocollo usato dai client di posta locali per recuperare i messaggi di posta elettronica dalle cassette postali con una connessione TCP/IP.
Rapporto di mancato recapito	Un messaggio di posta elettronica automatico inviato al mittente in caso di problemi nella consegna della posta.
RBL	Vedere Realtime Blocklist
Realtime Blocklist	Data base online di indirizzi IP spam. I messaggi di posta elettronica in entrata vengono messi a confronto con questi elenchi per stabilire se provengono da utenti presenti nelle black list.
Regole di monitoraggio dei messaggi di posta elettronica	Regole che consentono la replica di messaggi di posta elettronica tra indirizzi di posta elettronica.
Risposta automatica	Un messaggio di posta elettronica di risposta inviato automaticamente ai messaggi in entrata.
Secure Sockets Layer	Un protocollo inteso a garantire una comunicazione integrale e sicura tra le reti.
Server di elenco	Un uso particolare dei sistemi di posta elettronica che consente un'ampia distribuzione di messaggi a moltissimi utenti di posta elettronica attraverso liste di discussioni e newsletter.

Server/gateway perimetrale	Il computer (server) in un LAN direttamente connesso a una rete esterna. In GFI MailEssentials, il gateway perimetrale fa riferimento ai server di posta elettronica all'interno dell'azienda che ricevono per primi la posta elettronica dai domini esterni.
Simple Mail Transport Protocol	Uno standard Internet usato per la trasmissione di messaggi di posta elettronica attraverso le reti IP.
SMTP	Vedere Simple Mail Transport Protocol
SSL	Vedere Secure Sockets Layer
WebDAV	Un data base con estensione HTTP che consente agli utenti di gestire i file a distanza e in modo interattivo. Usato per la gestione della posta elettronica nella cassetta postale e nella cartella pubblica in Microsoft Exchange.
White list	Un elenco di indirizzi di posta elettronica e domini dai quali si desidera sempre ricevere messaggi di posta elettronica.
Zombie	*Vedere* Botnet
Zona demilitarizzata	Una sezione di una rete che non fa parte della rete interna e non fa parte direttamente di Internet. In genere, il suo scopo è agire come gateway tra le reti interne e Internet.

10 Indice

M

N

P

R

S

T

W