

# Guida alle best practice per i filtri antispam, antivirus, di posta grigia ed epidemie

## Sommario

[Panoramica](#)

[Antispam](#)

[Verifica chiave funzionalità](#)

[Abilita IMS \(Intelligent Multi-Scan\) a livello globale](#)

[Abilita quarantena della posta indesiderata centralizzata](#)

[Configura protezione da posta indesiderata nei criteri](#)

[Antivirus](#)

[Verifica tasti funzione](#)

[Abilita scansione antivirus](#)

[Configurare antivirus nei criteri di posta elettronica](#)

[Graymail](#)

[Verifica chiave funzionalità](#)

[Abilita i servizi di posta grigia e di cancellazione sicura dell'iscrizione](#)

[Configura la posta grigia e l'annullamento sicuro della sottoscrizione nei criteri](#)

[Filtri epidemie](#)

[Verifica chiave funzionalità](#)

[Abilita il servizio Filtri epidemie](#)

[Configurare i filtri epidemie nei criteri](#)

[Conclusioni](#)

## Panoramica

La maggior parte delle minacce, degli attacchi e dei disturbi affrontati da un'organizzazione tramite la posta elettronica si presenta sotto forma di spam, malware e attacchi misti. Cisco Email Security Appliance (ESA) include diverse tecnologie e funzionalità per bloccare queste minacce sul gateway prima che entrino nell'organizzazione. In questo documento vengono descritti gli approcci best practice per configurare i filtri antispam, antivirus, di posta grigia ed epidemie sul flusso di posta in entrata e in uscita.

## Antispam

La protezione antispam risolve una vasta gamma di minacce note, tra cui spam, phishing e attacchi zombie, oltre a minacce e-mail di breve durata, difficili da rilevare, di volume ridotto, come le [truffe "419"](#). Inoltre, la protezione antispam identifica minacce miste nuove ed in evoluzione, come gli attacchi di spam che distribuiscono contenuti dannosi tramite un URL di download o un eseguibile.

Cisco Email Security offre le seguenti soluzioni anti-spam:

- IronPort Anti-Spam Filtering (IPAS)

- Cisco Intelligent Multi-Scan Filtering (IMS)

È possibile concedere in licenza entrambe le soluzioni, ma solo una può essere utilizzata in una particolare policy di posta. Ai fini di questo documento, verrà utilizzata la funzionalità IMS.

## Verifica chiave funzionalità

- Sull'ESA, selezionare **System Administration > Feature Keys (Amministrazione sistema > Chiavi funzione)**
- Cercare la licenza Intelligent Multi-Scan e verificare che sia attiva.

## Abilita IMS (Intelligent Multi-Scan) a livello globale

- On OSPF (Open Shortest Path First) ESA, navigare a **Sicurezza Servizi > IMS e Graymail**
- Clic OSPF (Open Shortest Path First) **Attiva in Impostazioni globali IMS:**

IMS Global Settings	
Ironport Intelligent Multi-Scan:	Enabled
Regional Scanning:	Off
<a href="#">Edit IMS Settings</a>	

- Cerca **impostazioni globali comuni** e fare clic su **Modifica impostazioni globali**
- Qui tu puoi configurazione multiplo impostazioni. OSPF (Open Shortest Path First) consigliato impostazioni sono visualizzato in OSPF (Open Shortest Path First) immagine di seguito:

Edit Common Global Settings	
Message Scanning Thresholds:	<p>Increasing these values may result in decreased performance. Please consult documentation for size recommendations based on your environment.</p> <p>Always scan messages smaller than <input type="text" value="2M"/> Maximum  <small>Add a trailing K or M to indicate units. Recommended setting is 1024K(1MB) or less.</small></p> <p>Never scan messages larger than <input type="text" value="3M"/> Maximum  <small>Add a trailing K or M to indicate units. Recommended setting is 2048K(2MB) or less.</small></p>
Timeout for Scanning Single Message:	<input type="text" value="60"/> Seconds

- Fare clic su **Submit (Invia).**e **Conferma modifiche.**

Se non si dispone di una sottoscrizione di licenza IMS:

- Selezionare **Security Services > IronPort Anti-Spam**
- Clic OSPF (Open Shortest Path First) **Attiva pulsante** sulla **panoramica di IronPort Anti-Spam**
- Fare clic su **Modifica impostazioni globali**
- Qui tu puoi configurazione multiplo impostazioni. OSPF (Open Shortest Path First) consigliato impostazioni sono visualizzato in OSPF (Open Shortest Path First) immagine di seguito:

IronPort Anti-Spam Global Settings	
<input checked="" type="checkbox"/> <b>Enable IronPort Anti-Spam Scanning</b>	
Message Scanning Thresholds:	<p>Increasing these values may result in decreased performance. Please consult documentation for size recommendations based on your environment.</p> <p>Always scan messages smaller than <input type="text" value="2M"/> Maximum Add a trailing K or M to indicate units. Recommended setting is 1024K(1MB) or less.</p> <p>Never scan messages larger than <input type="text" value="3M"/> Maximum Add a trailing K or M to indicate units. Recommended setting is 2048K(2MB) or less.</p>
Timeout for Scanning Single Message:	<input type="text" value="60"/> Seconds
Scanning Profile:	<p><input type="radio"/> Normal</p> <p><input checked="" type="radio"/> <b>Aggressive</b> Recommended for customers who desire a stronger emphasis on blocking spam. When enabled, tuning Anti-Spam policy thresholds will have more impact on spam detection than the normal profile with a larger potential for false positives. Do not select the aggressive profile if IMS is enabled on the mail policy.</p> <p><input type="radio"/> Regional (China)</p>

- Cisco consiglia di selezionare il profilo di scansione **aggressiva** per i clienti che desiderano porre l'accento sul blocco della posta indesiderata.
- Fare clic su **Submit (Invia)**.e **Conferma modifiche**

## Abilita quarantena della posta indesiderata centralizzata

Dal momento che la funzionalità Protezione da posta indesiderata può essere impostata per essere messa in quarantena, è importante assicurarsi che tale funzionalità sia configurata:

- Passare a **Servizi di sicurezza > Quarantena posta indesiderata**
- Cliccare OSPF (Open Shortest Path First) **Configurazione** pulsante sarà prendere tu a OSPF (Open Shortest Path First) piegare debitore pagina.
- Qui tu puoi attivare OSPF (Open Shortest Path First) quarantena da controllo OSPF (Open Shortest Path First) **attivare** scatola e punto this quarantena a essere centralizzato on a) Sicurezza Gestione AApliance (SMA) dariempimento in SMANome e IP indirizzo. OSPF (Open Shortest Path First) consigliato impostazioni sono visualizzato di seguito:

External Spam Quarantine Settings	
<input checked="" type="checkbox"/> <b>Enable External Spam Quarantine</b>	
Name:	<input type="text" value="centralized_spam"/> (e.g. spam_quarantine)
IP Address:	<input type="text" value="sma_ip_address"/>
Port	<input type="text" value="6025"/>
Safelist/Blocklist:	<input checked="" type="checkbox"/> <b>Enable End User Safelist/Blocklist Feature</b> Blocklist Action: <input type="text" value="Quarantine"/>

- Fare clic su **Submit (Invia)**.e **Conferma modifiche**

Per ulteriori informazioni sull'impostazione e la centralizzazione delle quarantene, fare riferimento al documento sulle best practice:

[Procedure ottimali per la configurazione centralizzata di quarantene per virus ed epidemie e per la migrazione da ESA a SMA](#)

## Configura protezione da posta indesiderata nei criteri

Una volta Intelligente Multiplo - Scansione ha è stato configurato globalmente, tu puoi ora applicare Intelligente Multiplo - Scansione a posta criteri:

- Passare a **Criteri posta > Criteri posta in arrivo**

- Per impostazione predefinita, i criteri della posta in arrivo utilizzano le impostazioni di protezione da posta indesiderata IronPort.
- Se si fa clic sul collegamento blu in **Protezione antispam**, sarà possibile utilizzare le impostazioni personalizzate della protezione antispam per il criterio specifico.
- Di seguito è riportato un esempio che mostra i criteri predefiniti utilizzando le impostazioni personalizzate per la protezione dalla posta indesiderata:

Policies								
Order	Policy Name	Anti-Spam	Anti-Virus	Advanced Malware Protection	Graymail	Content Filters	Outbreak Filters	Delete
	Default Policy	IronPort Intelligent Multi-Scan Positive: Deliver Suspected: Deliver	Sophos Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop	File Reputation Malware File: Drop Pending Analysis: Quarantine Unscannable - Message Error: Deliver Unscannable - Rate Limit: Deliver Unscannable - AMP Service Not ... ...	Graymail Detection Unsubscribe: Enabled Marketing: Spam Quarantine Social: Spam Quarantine Bulk: Spam Quarantine ...	URL_LOG_ALL_REPUTATION URL_LOG_ALL_CATEGORY URL_QUARANTINE_MALICIOUS URL_REWRITE_SUSPICIOUS URL_INAPPROPRIATE SPF_DKIM_FAIL ...	Retention Time: Virus: 1 day Other: 4 hours	

Personalizzare le impostazioni della protezione dalla posta indesiderata per un criterio Posta in arrivo facendo clic sul collegamento blu in **Protezione dalla posta indesiderata** per il criterio che si desidera personalizzare.

Qui tu puoi selezionare OSPF (Open Shortest Path First) Anti-Spam Scansione opzione tu desiderio a attivare per questo policy.

- Per OSPF (Open Shortest Path First) scopi di questo migliore praticareghiaccio documento, fare clic OSPF (Open Shortest Path First) radio pulsante avanti a Utilizzo **IronPort Intelligent Multi-Scansione**:

Anti-Spam Settings	
<b>Policy:</b>	Default
Enable Anti-Spam Scanning for This Policy:	<input type="radio"/> Use IronPort Anti-Spam service <input checked="" type="radio"/> Use IronPort Intelligent Multi-Scan <i>Spam scanning built on IronPort Anti-Spam.</i> <input type="radio"/> Disabled

Le due sezioni successive includono **Impostazioni di posta indesiderata identificate in modo positivo** e **Impostazioni di posta indesiderata sospetta**:

- La procedura consigliata consiste nel configurare l'azione di **quarantena** sull'impostazione **Spam identificata positivamente** con il testo preceduto **[SPAM]** aggiunto all'oggetto e
- Applica a **recapita** come azione per **le impostazioni di posta indesiderata** con il testo anteposto **[SUSPECTED SPAM]** aggiunto all'oggetto:

Positively-Identified Spam Settings	
Apply This Action to Message:	Spam Quarantine <input type="button" value="v"/> <i>Note: If local and external quarantines are defined, mail will be sent to local quarantine.</i>
Add Text to Subject:	Prepend <input type="button" value="v"/> <input type="text" value="[SPAM]"/>
<input type="button" value="v"/> <b>Advanced</b>	Optional settings for custom header and message delivery.
Suspected Spam Settings	
Enable Suspected Spam Scanning:	<input type="radio"/> No <input checked="" type="radio"/> Yes
Apply This Action to Message:	Deliver <input type="button" value="v"/> Send to Alternate Host (optional): <input type="text"/>
Add Text to Subject:	Prepend <input type="button" value="v"/> <input type="text" value="[SUSPECTED SPAM]"/>
<input type="button" value="v"/> <b>Advanced</b>	Optional settings for custom header and message delivery.

- È possibile modificare l'impostazione della **soglia della posta indesiderata**; le impostazioni consigliate sono la personalizzazione del punteggio **Identificato in modo positivo** a **90** e del

punteggio **Sospetto posta indesiderata** a **43**:

Spam Thresholds	
<i>Spam is scored on a 1-100 scale. The higher the score, the more likely a message is a spam.</i>	
IronPort Anti-Spam:	<input checked="" type="radio"/> Use the Default Thresholds <input type="radio"/> Use Custom Settings: Positively Identified Spam: Score > <input type="text" value="90"/> (50 - 100) Suspected Spam: Score > <input type="text" value="50"/> (minimum 25, cannot exceed positive spam score)
IronPort Intelligent Multi-Scan:	<input type="radio"/> Use the Default Thresholds <input checked="" type="radio"/> Use Custom Settings: Positively Identified Spam: Score > <input type="text" value="90"/> (50 - 100) Suspected Spam: Score > <input type="text" value="43"/> (minimum 25, cannot exceed positive spam score)

- Fare clic su **Submit (Invia)**.e **Conferma modifiche**

## Antivirus

La protezione antivirus è fornita da due motori di terze parti, Sophos e McAfee. Questi motori filtreranno tutte le minacce maligne conosciute, rilasciandole, pulendole o mettendole in quarantena come configurato.

## Verifica tasti funzione

Per verificare che entrambe le chiavi di funzionalità siano attivate:

- Selezionare **Amministrazione sistema > Tasti funzione**
- Accertarsi che le licenze **Sophos Anti-Virus** e **McAfee** siano attive.

## Abilita scansione antivirus

- Naviga a **Sicurezza Servizi> Antivirus - Sophos**
- Clic OSPF (Open Shortest Path First) **Attivapulsante**.
- Verificare che l'opzione **Aggiornamento automatico** sia **attivata** e che l'aggiornamento dei file antivirus Sophos funzioni correttamente. Se necessario, fare clic su **Aggiorna ora** per avviare immediatamente l'aggiornamento del file:

Sophos Anti-Virus Overview	
Anti-Virus Scanning by Sophos Anti-Virus:	Enabled
Virus Scanning Timeout (seconds):	60
Automatic Updates: (?)	Enabled
<a href="#">Edit Global Settings...</a>	

Current Sophos Anti-Virus files			
File Type	Last Update	Current Version	New Update
Sophos Anti-Virus Engine	Wed Nov 6 10:04:30 2019	3.2.07.377.1_5.68	Not Available
Sophos IDE Rules	Wed Nov 6 12:03:56 2019	2019110602	Not Available
No updates in progress.			
<a href="#">Update Now</a>			

- Fare clic su **Submit (Invia)**.e **Conferma modifiche**.

Se è attiva anche la licenza McAfee, selezionare a **Sicurezza Servizi> Antivirus - McAfee**

- Clic OSPF (Open Shortest Path First) **Attivapulsante**.

- Verificare che **Aggiornamento automatico** sia **abilitato** e che l'aggiornamento dei file di McAfee Anti-Virus funzioni correttamente. Se necessario, fare clic su **Aggiorna ora** per avviare immediatamente l'aggiornamento del file.
- Fare clic su **Submit (Invia)** e **Conferma modifiche**

## Configurare antivirus nei criteri di posta elettronica

In un criterio Posta in arrivo è consigliabile eseguire le operazioni seguenti:

- Passare a **Criteri posta > Criteri posta in arrivo**
- Personalizzare le impostazioni **antivirus** per un criterio posta in arrivo facendo clic sul collegamento blu in Antivirus per il criterio che si desidera personalizzare.
- Qui tu puoi selezionare OSPF (Open Shortest Path First) Anti-Virus Scansione opzione tu desiderio a attivare per questo policy.
- Per OSPF (Open Shortest Path First) scopi di questa bconfigurare scattoghiaccio selezionare **McAfee e Sophos Anti-Virus**:

Anti-Virus Settings	
<b>Policy:</b>	DEFAULT
<b>Enable Anti-Virus Scanning for This Policy:</b>	<input checked="" type="radio"/> Yes <input checked="" type="checkbox"/> Use McAfee Anti-Virus <input checked="" type="checkbox"/> Use Sophos Anti-Virus <input type="radio"/> No

- Non si tenta di ripristinare un file, quindi l'analisi dei messaggi rimane **Solo ricerca virus**:

Message Scanning	
	Scan for Viruses only <input type="button" value="v"/> <input type="checkbox"/> Drop infected attachments if a virus is found <input checked="" type="checkbox"/> (recommended) Include an X-header with the Anti-Virus scanning results in messages
Repaired Messages:	
Action Applied to Message:	<input type="text" value="Deliver As Is"/>
Archive Original Message:	<input checked="" type="radio"/> No <input type="radio"/> Yes
Modify Message Subject:	<input checked="" type="radio"/> No <input type="radio"/> Prepend <input type="radio"/> Append
	<input type="text" value="[WARNING: VIRUS REMOVED]"/>
<a href="#">Advanced</a>	Optional settings for custom header and message delivery.

- L'azione consigliata per i **messaggi crittografati e non scansionabili** è **recapitare** il messaggio così com'è modificando l'oggetto.
- Il criterio consigliato per Antivirus è **Elimina** tutti i **messaggi infetti da virus**, come mostrato nell'immagine seguente:

Encrypted Messages:	
Action Applied to Message:	Deliver As Is
Archive Original Message:	<input checked="" type="radio"/> No <input type="radio"/> Yes
Modify Message Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append
	[A/V UNSCANNABLE]
▶ Advanced	Optional settings for custom header and message delivery.
Unscannable Messages:	
Action Applied to Message:	Deliver As Is
Archive Original Message:	<input checked="" type="radio"/> No <input type="radio"/> Yes
Modify Message Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append
	[A/V UNSCANNABLE]
▶ Advanced	Optional settings for custom header and message delivery.
Virus Infected Messages:	
Action Applied to Message:	Drop Message
Archive Original Message:	<input checked="" type="radio"/> No <input type="radio"/> Yes
Modify Message Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append
	[WARNING : VIRUS DETECTED]
▶ Advanced	Optional settings for custom header and message delivery.

- Fare clic su **Submit (Invia)** e **Conferma modifiche**

Un criterio simile è consigliato per i criteri Posta in uscita, tuttavia si sconsiglia di modificare l'oggetto della posta in uscita.

## Graymail

La soluzione di gestione delle e-mail di Greymail Security Appliance è costituita da due componenti: un motore di scansione della posta grigia integrato e un servizio Unsubscribe basato su cloud. La soluzione di gestione della posta grigia consente alle organizzazioni di identificare la posta grigia utilizzando il motore di posta grigia integrato e di applicare i controlli di policy appropriati e fornire un meccanismo semplice agli utenti finali per annullare la sottoscrizione ai messaggi indesiderati utilizzando il servizio di annullamento della sottoscrizione.

Le categorie di posta grigia includono marketing, social network e posta elettronica in blocco. Le opzioni avanzate includono l'aggiunta di un'intestazione personalizzata, l'invio a un host alternativo e l'archiviazione del messaggio. Per questa procedura ottimale, abilitiamo la funzione di annullamento della sottoscrizione sicura di Graymail per il criterio di posta predefinito.

### Verifica chiave funzionalità

- Sull'ESA, selezionare **System Administration > Feature Keys (Amministrazione sistema > Chiavi funzione)**
- Cercare **GreyMail Safe Unsubscription** e assicurarsi che sia attivo.

### Abilita i servizi di posta grigia e di cancellazione sicura dell'iscrizione

- On OSPF (Open Shortest Path First) ESA, navigare a **Sicurezza Servizi > IMS e Graymail**
- Clic OSPF (Open Shortest Path First) **Modifica impostazioni posta grigia** pulsante in **Impostazioni globali di Graymail**
- Selezionare tutte le opzioni - **Attiva rilevamento posta grigia, Attiva annullamento sicuro**

## sottoscrizione e Attiva aggiornamenti automatici:

Graymail Global Settings	
Graymail Detection	Enabled
Safe Unsubscribe	Enabled
Automatic Updates ?	Enabled

[Edit Graymail Settings](#)

- Fare clic su **Submit (Invia)** e **Conferma modifiche**

## Configura la posta grigia e l'annullamento sicuro della sottoscrizione nei criteri

Once, Greymail e l'annullamento sicuro dell'iscrizione ha è stato configurato globalmente , tu può ora applica questi servizi a posta politiche.

- Passare a **Criteri posta > Criteri posta in arrivo**
- Se si fa clic sul collegamento blu in **Greymail**, per quel particolare criterio sarà possibile usare le impostazioni di Greymail personalizzate.
- Qui tu può selezionare Graymail opzioni tu desiderio a attivare per questo policy.
- Per OSPF (Open Shortest Path First) scopi di questo p  
ottimalescattoghiaccio documento, fare clic OSPF (Open Shortest Path  
First) radio pulsante avanti per **abilitare il rilevamento della posta grigia per questo criterio e  
abilitare l'annullamento della sottoscrizione della posta grigia per questo criterio:**

Graymail Settings	
<b>Policy:</b>	DEFAULT
<b>Enable Graymail Detection for This Policy:</b>	<input checked="" type="radio"/> Yes <input type="radio"/> No
<b>Enable Graymail Unsubscribing for This Policy:</b>	<input checked="" type="radio"/> Yes <input type="radio"/> No
	Perform this action for: <input checked="" type="radio"/> All Messages (Recommended) <input type="radio"/> Unsigned Messages

Le tre sezioni successive includono **Azione sulle impostazioni di posta elettronica di marketing**, **Azione sulle impostazioni di posta elettronica dei social network** e **Azione sulle impostazioni di posta elettronica di massa**.

- La migliore pratica raccomandata è di abilitarli tutti e rimanere l'azione come **Consegna** con testo preceduto aggiunto al soggetto in relazione alle categorie come mostrato di seguito:



✓ Action on Marketing Email	
Apply this action to Message:	Deliver <input type="button" value="↓"/> Send to Alternate Host (optional): <input type="text"/>
Add Text to Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append <input type="text" value="[MARKETING]"/>
▶ Advanced	<i>Optional settings for custom header and message delivery.</i>
✓ Action on Social Network Email	
Apply this action to Message:	Deliver <input type="button" value="↓"/> Send to Alternate Host (optional): <input type="text"/>
Add Text to Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append <input type="text" value="[SOCIAL NETWORK]"/>
▶ Advanced	<i>Optional settings for custom header and message delivery.</i>
✓ Action on Bulk Email	
Apply this action to Message:	Deliver <input type="button" value="↓"/> Send to Alternate Host (optional): <input type="text"/>
Add Text to Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append <input type="text" value="[BULK]"/>
▶ Advanced	<i>Optional settings for custom header and message delivery.</i>

- Fare clic su **Submit (Invia)**.e **Conferma modifiche**

La condizione **Graymail** dei criteri della posta in uscita deve rimanere **disabilitata**.

## Filtri epidemie

I filtri epidemie combinano trigger nel motore antispam, tecnologie di scansione e rilevamento degli URL e altro ancora per etichettare correttamente gli elementi che non rientrano nella vera categoria di posta indesiderata, come ad esempio le e-mail di phishing e di truffa, e li gestiscono in modo appropriato con le notifiche degli utenti o la quarantena.

### Verifica chiave funzionalità

- Sull'ESA, selezionare **System Administration > Feature Keys (Amministrazione sistema > Chiavi funzione)**
- Cercare i **filtri epidemie** e verificare che sia attivo.

### Abilita il servizio Filtri epidemie

- On OSPF (Open Shortest Path First) ESA, navigare a **Sicurezza Servizi> Filtri epidemie**
- Clic OSPF (Open Shortest Path First) **Attivapulsante Panoramica dei filtri epidemie**
- Qui tu può configurazione multiplo impostazioni. OSPF (Open Shortest Path First) consigliato impostazioni sono visualizzato in OSPF (Open Shortest Path First) immagine di seguito:

Outbreak Filters Global Settings	
<input checked="" type="checkbox"/> <b>Enable Outbreak Filters</b>	
Adaptive Rules:	<input checked="" type="checkbox"/> <b>Enable Adaptive Rules</b>
Maximum Message Size to Scan:	<input type="text" value="3M"/> Maximum <i>Add a trailing K or M to indicate units.</i>
Emailed Alerts: ?	<input checked="" type="checkbox"/> <b>Receive Emailed Alerts</b>
Web Interaction Tracking: ?	<input checked="" type="checkbox"/> <b>Enable Web Interaction Tracking</b>

- Fare clic su **Submit (Invia)**.e **Conferma modifiche**.

## Configurare i filtri epidemie nei criteri

Filtri epidemie una sola volta ha è stato configurato globalmente , tu può ora applica questa funzionalità a posta politiche.

- Passare a **Criteri posta > Criteri posta in arrivo**
- Se si fa clic sul collegamento blu in **Filtri epidemie**, sarà possibile usare le impostazioni personalizzate dei filtri epidemie per quel criterio specifico.
- Per OSPF (Open Shortest Path First) scopi di questo migliore praticare ghiaccio , le impostazioni del filtro epidemie vengono mantenute con i valori predefiniti:

Outbreak Filter Settings	
Quarantine Threat Level: ?	<input type="text" value="3"/>
Maximum Quarantine Retention:	Viral Attachments: <input type="text" value="1"/> <input type="text" value="Days"/>
	Other Threats: <input type="text" value="4"/> <input type="text" value="Hours"/>
	<input type="checkbox"/> Deliver messages without adding them to quarantine
Bypass Attachment Scanning: ▶	None configured

- I filtri epidemie possono riscrivere gli URL se vengono considerati dannosi, sospetti o phishing. Selezionare **Abilita modifica messaggi** per rilevare e riscrivere le minacce basate su URL.
- Verificare che l'opzione **URL Rewriting** (Riscrittura URL) sia **Abilita** per tutti i messaggi, come mostrato di seguito:

Message Modification	
<input checked="" type="checkbox"/> <b>Enable message modification. Required for non-viral threat detection (excluding attachments)</b>	
Message Modification Threat Level: ?	<input type="text" value="3"/>
Message Subject:	Prepend <input type="text" value="[Possible \$threat_category Fraud]"/> <a href="#">Insert Variables</a>   <a href="#">Preview Text</a>
Include the X-IronPort-Outbreak-Status headers:	<input type="radio"/> Enable for all messages <input type="radio"/> Enable only for threat-based outbreak <input checked="" type="radio"/> <b>Disable</b>
Include the X-IronPort-Outbreak-Description header:	<input type="radio"/> Enable <input checked="" type="radio"/> <b>Disable</b>
Alternate Destination Mail Host (Other Threats only):	<input type="text"/> <i>(examples: example.com, 10.0.0.1, 2001:420:80:1::5)</i>
URL Rewriting:	Cisco Security proxy scans and rewrites all URLs contained in malicious outbreak emails. <input type="radio"/> Enable only for unsigned messages (recommended) <input checked="" type="radio"/> <b>Enable for all messages</b> <input type="radio"/> Disable
	Bypass Domain Scanning ? <input type="text"/> <i>(examples: example.com, crm.example.com, 10.0.0.1, 10.0.0.0/24, 2001:420:80:1::5, 2001:db8::/32)</i>
Threat Disclaimer:	<input type="text" value="System Generated"/> <a href="#">Preview Disclaimer</a> <i>Disclaimer text will be applied to the top of the message body for Suspicious and Quarantined messages. To create custom disclaimers go to Mail Policies &gt; Text Resources &gt; Disclaimers</i>

- Fare clic su **Submit (Invia)**.e **Conferma modifiche**

Nei criteri di posta in uscita i **filtri epidemie** devono rimanere **disabilitati**.

## Conclusioni

Questo documento ha lo scopo di descrivere le configurazioni predefinite, o best practice, per i filtri antispam, antivirus, grigi ed epidemie di Email Security Appliance (ESA). Tutti questi filtri sono disponibili sia nei criteri della posta in arrivo che in uscita, e la configurazione e il filtro sono consigliati su entrambi - mentre la maggior parte della protezione è per il traffico in entrata, il filtro del flusso in uscita fornisce protezione dai messaggi inoltrati o da attacchi dannosi interni.