Come archiviare le e-mail su Email Security Appliance e Cloud Email Security?

Sommario

Introduzione

Questo documento descrive i passaggi da seguire per archiviare le e-mail su Email Security Appliance (ESA) e Cloud Email Security (CES) per il recupero e la revisione.

Premesse

Quando si archiviano messaggi di posta elettronica su ESA e CES, è possibile utilizzarli per soddisfare i requisiti normativi o per fornire un ulteriore mezzo di dati per un'ulteriore diagnosi e revisione della posta. L'archiviazione dei messaggi di posta elettronica funge da archiviazione secondaria dei messaggi di posta elettronica in formato di registro casella postale nell'origine originale e consente agli amministratori di recuperarli e convalidarli.

- Si consiglia di mantenere le impostazioni ai valori predefiniti se si decide di abilitare l'archiviazione dei messaggi di posta elettronica. I valori predefiniti sono 10 MB per registro e 10 registri mantenuti al massimo. I registri continueranno ad essere aggiunti e sottoposti a rollover in base alle dimensioni del file di registro stesso. I file di registro della casella di posta dell'archivio vengono riempiti in base alla frequenza del traffico di posta elettronica che passa attraverso l'accessorio. Man mano che vengono creati altri log, i log della casella di posta di archivio meno recenti vengono rimossi per liberare spazio per la creazione del nuovo log.
- Verificare che il dispositivo disponga di spazio su disco sufficiente prima di aumentare le dimensioni del file di registro della cassetta postale di archivio e di mantenere il numero massimo di file di registro.
- Per interrompere la generazione dei log della casella di posta dell'archivio, è necessario disabilitare la funzione di archivio in base ai criteri.

Nota: I log delle caselle di posta dell'archivio ESA e CES non possono essere recuperati da Security Management Appliance (SMA) e vengono memorizzati localmente per ciascuna

ESA e CES con la funzione abilitata.

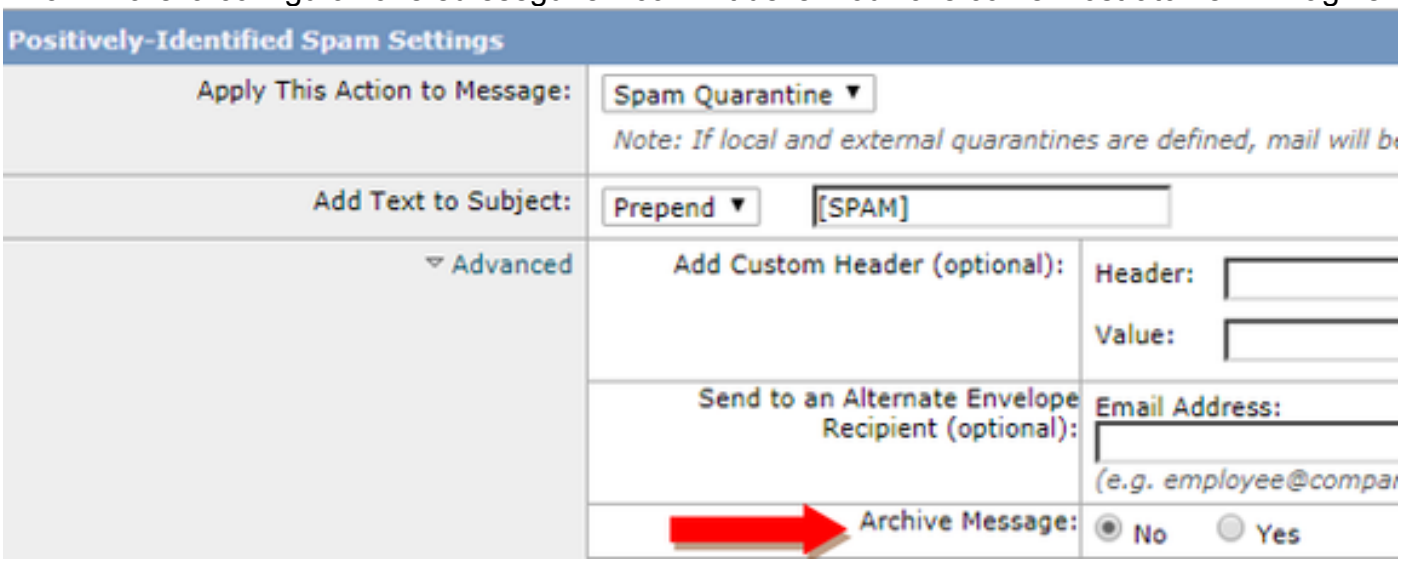
Come archiviare le e-mail su ESA e CES?

L'archiviazione della posta elettronica è disponibile con i filtri antispam, antivirus, protezione avanzata da malware, posta grigia e messaggi. L'azione di archiviazione può essere configurata tramite l'interfaccia grafica utente (GUI) o l'interfaccia della riga di comando (CLI) per la protezione da posta indesiderata, antivirus, antimalware avanzata e Graymail.

Per i filtri messaggi, l'azione di archiviazione può essere configurata utilizzando solo la CLI.

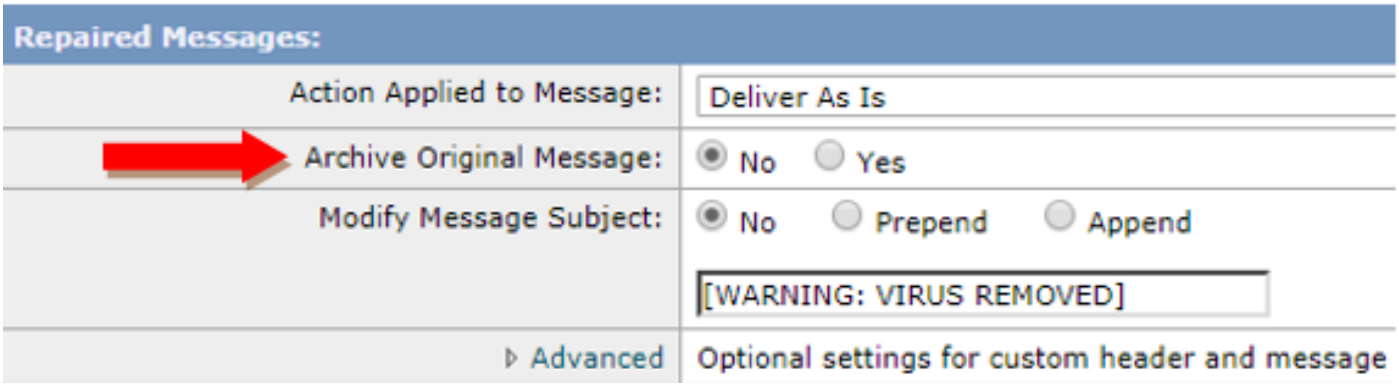
Configura archivio posta indesiderata

1. Selezionare **GUI > Mail Policies > Incoming/Outgoing Mail Policies** (Policy di posta > Criteri posta in arrivo/in uscita).
2. Per configurare l'archiviazione della posta elettronica, fare clic sulle impostazioni della protezione da posta indesiderata per il criterio corrispondente.
3. Fare clic su **Advanced** (Avanzate) nelle impostazioni disponibili per Positive Identified Spam Settings (Impostazioni posta indesiderata identificata positivamente) e/o Suspected Spam settings (Impostazioni sospette di posta indesiderata).
4. Premere il pulsante di opzione accanto a Sì per archiviare le e-mail con il verdetto antispam corrispondente.
5. Inviare la configurazione ed eseguire il commit delle modifiche come mostrato nell'immagine.



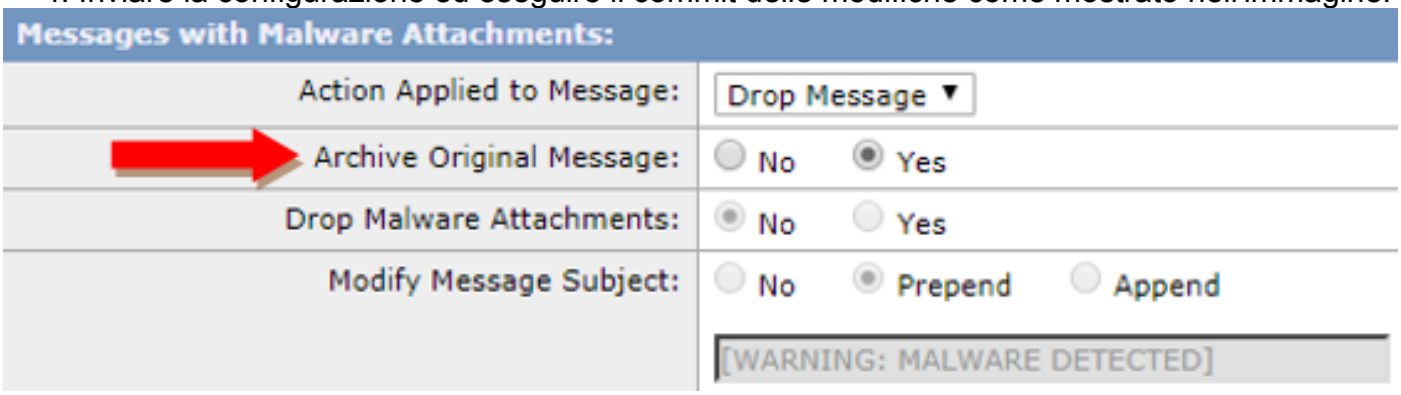
Configura archivio antivirus

1. Selezionare **GUI > Mail Policies > Incoming/Outgoing Mail Policies** (Policy di posta > Criteri posta in arrivo/in uscita).
2. Fare clic sulle impostazioni antivirus nei rispettivi criteri per configurare l'archiviazione della posta elettronica.
3. Su ciascuno dei verdetti di scansione che si desidera archiviare il messaggio originale, premere il pulsante di opzione accanto a Sì per archiviare.
4. Inviare la configurazione ed eseguire il commit delle modifiche come mostrato nell'immagine.



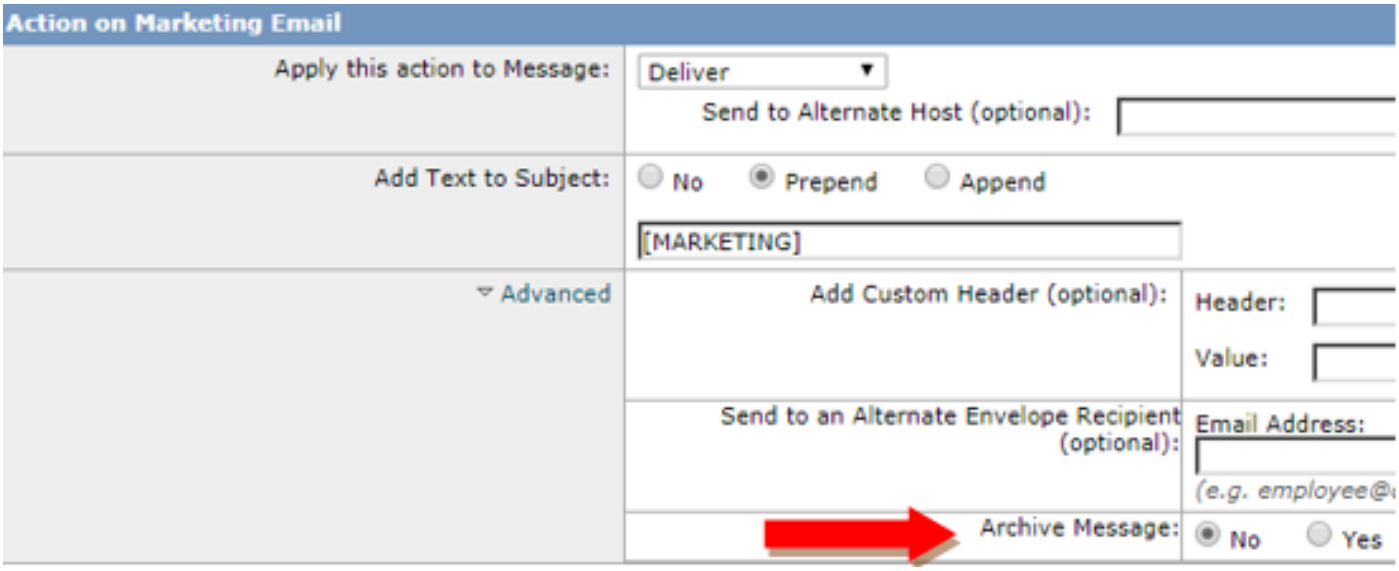
Configura Archivio Advanced Malware Protection

1. Selezionare **GUI > Mail Policies > Incoming/Outgoing Mail Policies** (Policy di posta > Criteri posta in arrivo/in uscita).
2. Per configurare l'archiviazione della posta elettronica, fare clic sulle impostazioni di Protezione avanzata da malware nei rispettivi criteri.
3. Su ciascuno dei verdetti di scansione che si desidera per archiviare il messaggio originale, premere il pulsante di opzione accanto a Sì per archiviare.
4. Inviare la configurazione ed eseguire il commit delle modifiche come mostrato nell'immagine.



Configura archivio di posta grigia

1. Selezionare **GUI > Mail Policies > Incoming/Outgoing Mail Policies** (Policy di posta > Criteri posta in arrivo/in uscita).
2. Per configurare l'archiviazione della posta elettronica, fare clic sulle impostazioni di Greymail nei rispettivi criteri.
3. Fare clic su Avanzate nelle impostazioni disponibili per Marketing, Social, Bulk.
4. Premere il pulsante di opzione accanto a Sì per archiviare le e-mail con il rispettivo verdetto di Graymail.
5. Inviare la configurazione ed eseguire il commit delle modifiche.



Configura archivio filtro messaggi

> **Nota**: per visualizzare i log archiviati è necessario un filtro messaggi con azione di archiviazione. i filtri messaggi possono essere creati solo nella CLI.

Filtro di esempio:

```
Test_Archive:
if (mail-from == "test1@cisco.com")
{
archive("Test");
}
```

1. Accedere al dispositivo dalla CLI.
2. Creare un filtro messaggi come indicato nel filtro di esempio fornito.
3. Inviare il filtro ed eseguire il commit delle modifiche.

Convalida disponibilità log della casella di posta dell'archivio

Quando viene eseguito il commit della configurazione per l'archivio per i rispettivi servizi, i messaggi di posta elettronica archiviati vengono archiviati in un file registro in formato mbox. Per verificare se i log di archivio sono disponibili per il recupero, selezionare **GUI > Amministrazione sistema > Sottoscrizioni log**.

Gli archivi dei servizi di sicurezza creano un log separato con un tipo di log di archivio come mostrato nell'immagine:

Configured Log Subscriptions

Add Log Subscription...

Log Settings	Type ▲	Log Files	Rollover Interval
amp	AMP Engine Logs	amp/	None
amparchive	AMP Archive	amparchive/	None
antispam	Anti-Spam Logs	antispam/	None
antivirus	Anti-Virus Logs	antivirus/	None
asarchive	Anti-Spam Archive	asarchive/	None
authentication	Authentication Logs	authentication/	None
avarchive	Anti-Virus Archive	avarchive/	None

Per i filtri messaggi, la configurazione dell'archivio viene visualizzata **solo** dalla **CLI**:

- **filtri > configurazione log**

```
demigod.cisco.com> filters

Choose the operation you want to perform:
- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.
[]> logconfig

Currently configured logs:
    Log Name          Log Type                    Retrieval          Interval
 ------------------------------------------------------------------------------
 1. Test              Filter Archive Logs         Manual Download    None
```

Recuperare i log delle caselle di posta

Per gli accessori standalone, questi registri mbox possono essere recuperati direttamente dalla GUI. Selezionare **GUI > Amministrazione di sistema >** Sottoscrizioni **log** e fare clic sui **file di log** per il log di archivio che verrà recuperato.

Per gli accessori in cluster, i registri mbox possono essere recuperati utilizzando il protocollo FTP/Secure Copy (SCP), come descritto in questo articolo. (https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118315-technote-esa-00...)

Informazioni correlate

- Cisco Email Security Appliance - Guide per l'utente
- Cos'è il formato mbox (mailbox) di UNIX?
- Dove e come posso accedere ai log archiviati su Cisco Email Security Appliance (ESA)
- Come estrarre un'e-mail dai log della casella di posta dell'archivio
- Documentazione e supporto tecnico – Cisco Systems