¿Cómo archivar los correos electrónicos en el dispositivo de seguridad y la nube del correo electrónico envíe por correo electrónico la Seguridad?

Contenido

Introducción

Este documento describe los pasos que se seguirán para archivar los correos electrónicos en la Seguridad del correo electrónico del dispositivo de seguridad (ESA) y de la nube del correo electrónico (CES) para la extracción y el estudio.

Antecedentes

Cuando usted archiva los correos electrónicos en el ESA y el CES, puede ser utilizado para cumplir los requisitos de regla o para proporcionar los medios adicionales de los datos para la diagnosis y el estudio adicionales del correo. El archivar envía por correo electrónico actúa como almacenamiento secundario de los correos electrónicos en un formato de registro del mbox en él es fuente original para los administradores para extraer y validar.

- Se recomienda para guardar las configuraciones a los valores predeterminados si usted decide habilitar archivar de los correos electrónicos. Los valores predeterminados son 10MB por el máximo del registro y de 10 registros conservado. Los registros continuarán siendo agregados y siendo rodados encima basado en el tamaño del archivo del registro sí mismo. Se llenan los archivos del registro del mbox del archivo basaron en el índice del tráfico del correo electrónico que pasa sin embargo el dispositivo. Mientras que se crean más registros, registros más viejos del mbox del archivo se quitan al espacio libre para la creación del nuevo registro.
- Asegúrese de que su dispositivo tenga suficiente espacio en disco antes de que usted aumente los tamaños de archivo de registro del mbox del archivo y los archivos del registro

máximos conservados.
- Para parar los registros del mbox del archivo de la generación, usted tendrá que inhabilitar la función del archivo por la directiva.

Note: Los registros del mbox del archivo ESA y CES no se pueden extraer por el S A y se salvan localmente por cada ESA y CES con la característica habilitada.

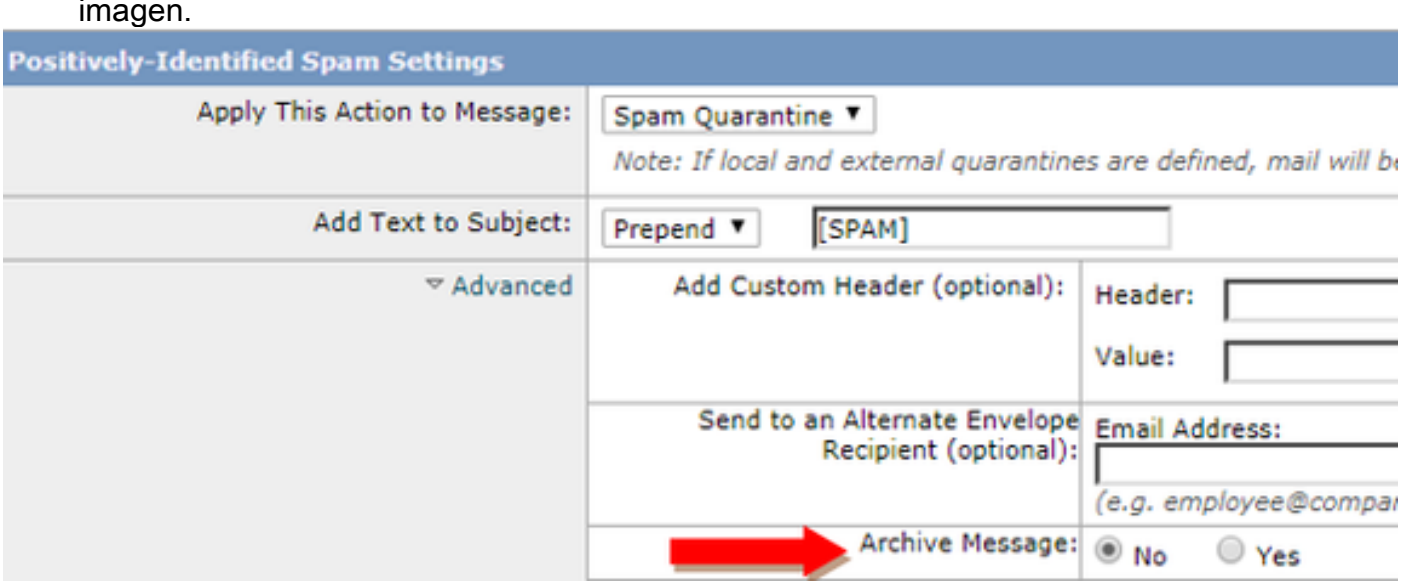
¿Cómo archivar los correos electrónicos en el ESA y el CES?

El archivar del correo electrónico está disponible con el Anti-Spam, el contra virus, los filtros avanzados de la protección de Malware, de Graymail y del mensaje. La acción del archivo se puede configurar en el GUI y el CLI para el Anti-Spam, el contra virus, la protección avanzada de Malware y Graymail.

La acción del archivo se puede configurar en el CLI solamente para los filtros del mensaje.

Archivo del Anti-Spam de la configuración

1. Navegue al **GUI > las directivas del correo > las directivas entrantes/salientes del correo**.
2. Haga clic en las configuraciones del Anti-Spam en la directiva respectiva para configurar archivar del email.
3. Haga clic **avanzado** en las configuraciones disponibles para las configuraciones positivamente identificadas del Spam, las configuraciones sospechosas del Spam.
4. Presione el botón de radio al lado del sí para archivar los correos electrónicos con el veredicto respectivo del Anti-Spam.
5. La configuración de Submitthe, y confía estos cambios tal y como se muestra en de la imagen.

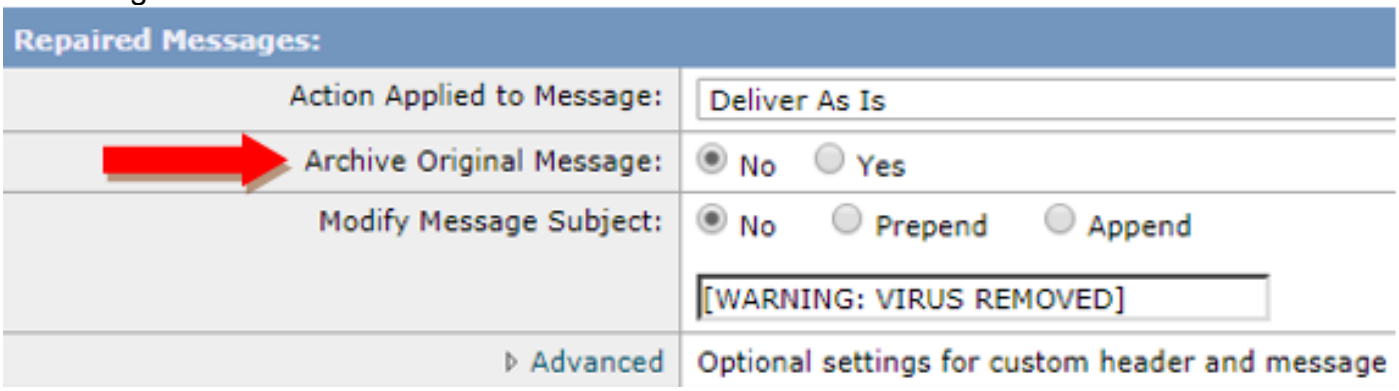


Archivo del contra virus de la configuración

1. Navegue al **GUI > las directivas del correo > las directivas entrantes/salientes del correo**.
2. Haga clic en las configuraciones del contra virus en la directiva respectiva para configurar archivar del email.
3. En cada uno de la exploración los veredictos que usted desea archivar el mensaje original,

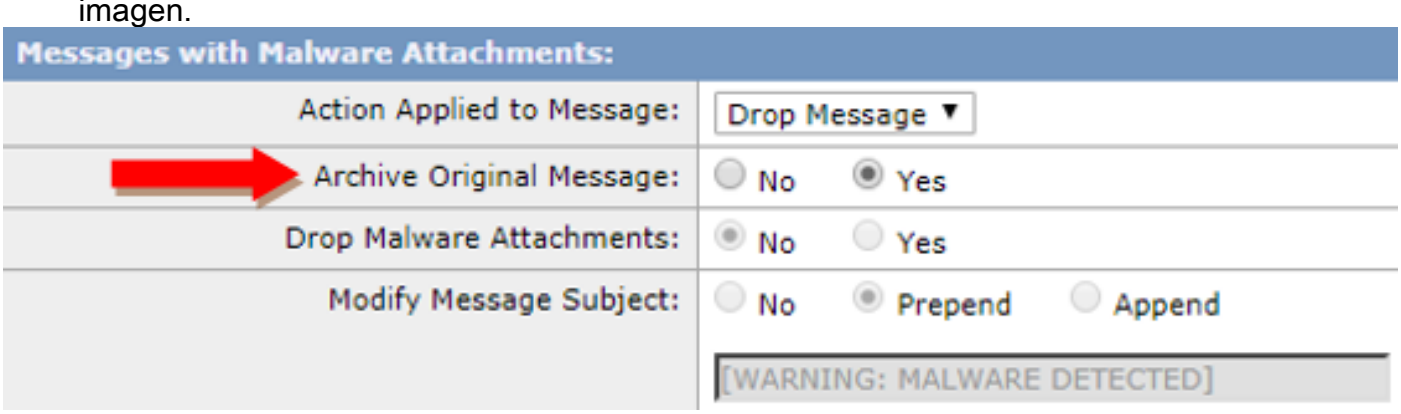
presionan el botón de radio al lado del sí en el archivo del orderto.

4. La configuración de Submitthe, y confía estos cambios tal y como se muestra en de la imagen.



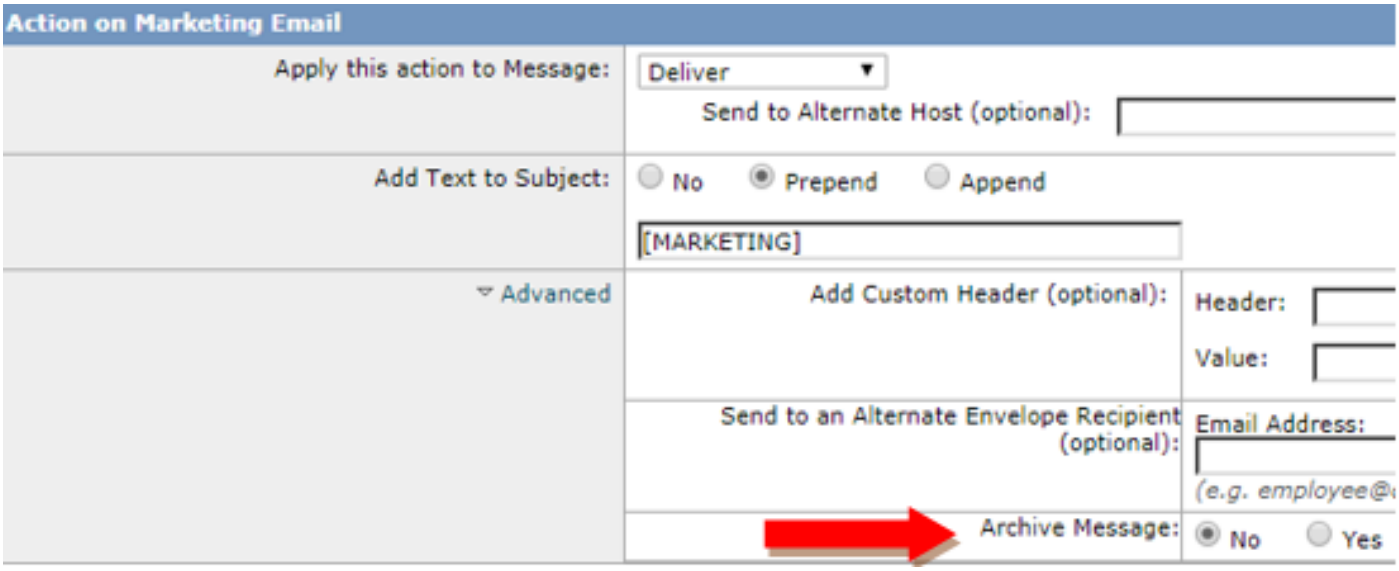
Archivo avanzado de la protección de Malware de la configuración

1. Navegue al **GUI > las directivas del correo > las directivas entrantes/salientes del correo**.
2. Haga clic en el Malware avanzado Protectionsettings en la directiva respectiva para configurar archivar del email.
3. En cada uno de la exploración los veredictos que usted desea para archivar el mensaje original, presionan el botón de radio al lado del sí para archivar.
4. La configuración de Submitthe, y confía estos cambios tal y como se muestra en de la imagen.



Archivo de Graymail de la configuración

1. Navegue al **GUI > las directivas del correo > las directivas entrantes/salientes del correo**.
2. Haga clic en las configuraciones de Graymail en la directiva respectiva para configurar archivar del email.
3. Haga clic **Advancedon las** configuraciones disponibles para comercializar, Social, bulto.
4. Presione el botón de radio al lado del sí para archivar los correos electrónicos con el veredicto respectivo de Graymail.
5. Someta la configuración, y confíe estos cambios.



Configure el archivo del filtro del mensaje

> **Note**: Un filtro del mensaje con la acción del archivo se requiere para ver los registros archivados. Los filtros del mensaje se pueden crear solamente dentro del CLI.

Filtro de la muestra:

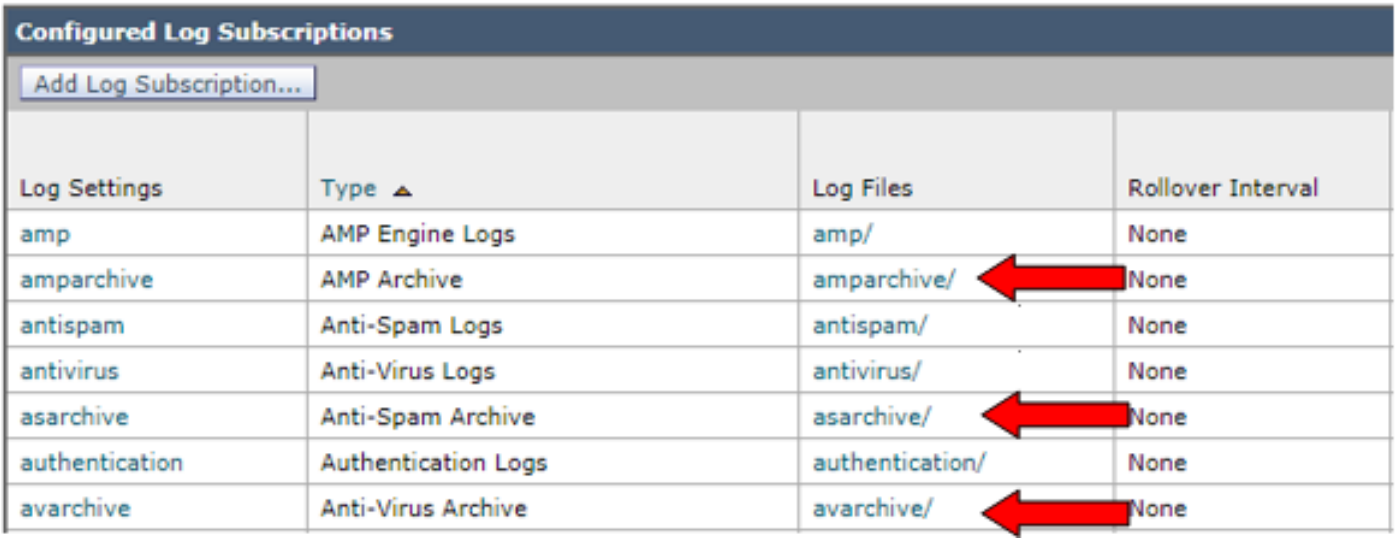
```
Test_Archive:
if (mail-from == "test1@cisco.com")
{
archive("Test");
}
```

1. Login al dispositivo en el CLI.
2. Cree un filtro del mensaje como se ve en el filtro de la muestra proporcionado.
3. Someta este filtro y confíe sus cambios.

Valide la Disponibilidad de los registros de Mbox del archivo

Cuando la configuración para el archivo está confiada para los servicios respectivos, los correos electrónicos archivados se salvan en un archivo del registro del formato del mbox. Para verificar si los registros del archivo están disponibles para la extracción, navegue al **GUI > las suscripciones de la administración del sistema > del registro**.

Los archivos de los Servicios de seguridad crean un registro separado con un tipo del registro del archivo tal y como se muestra en de la imagen:



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

Para el mensaje filtra la configuración del archivo se ve del **CLI solamente**:

- **filtros > logconfig**

```
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
```

Extraiga los registros de Mbox

Para los dispositivos independientes estos registros del mbox se pueden extraer directamente del GUI. Navegue al theGUI **> a la administración del sistema > al registro Subscriptionsand** hacen clic en los **archivos del registro** para el registro del archivo respectivo que usted extraerá.

Para los dispositivos agrupados, los registros del mbox se pueden extraer con el uso de la copia FTP/Secure (SCP) según lo descrito en el [thisarticle](https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118315-technote-esa-00....).
([https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118315-technote-esa-00....)](https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118315-technote-esa-00....)

Información Relacionada

- [Dispositivo de seguridad del correo electrónico de Cisco - Guías del usuario final]
- [¿Cuál es formato del mbox de UNIX (buzón)?]
- [Donde están los registros salvados en el dispositivo de seguridad del correo electrónico de Cisco (ESA) y cómo los accedo]
- [Cómo extraer un correo electrónico de los registros del mbox del archivo]

- Soporte Técnico y Documentación - Cisco Systems