

¿Cómo se archivan los correos electrónicos en Email Security Appliance y Cloud Email Security?

Contenido

[Introducción](#)

[Antecedentes](#)

[¿Cómo se archivan los correos electrónicos en ESA y CES?](#)

[Configuración del archivo Anti-Spam](#)

[Configurar el archivo antivirus](#)

[Configuración del archivo de protección frente a malware avanzado](#)

[Configurar el archivo de graymail](#)

[Configurar archivo de filtro de mensajes](#)

[Validar disponibilidad de registros Mbox de archivo](#)

[Recuperar los registros de Mbox](#)

[Información Relacionada](#)

Introducción

Este documento describe los pasos a seguir para archivar correos electrónicos en Email Security Appliance (ESA) y Cloud Email Security (CES) para su recuperación y revisión.

Antecedentes

Cuando archiva correos electrónicos en el ESA y el CES, se puede utilizar para cumplir los requisitos de la normativa o para proporcionar un medio adicional de datos para un diagnóstico y revisión posteriores del correo. El archivado de correos electrónicos actúa como un almacenamiento secundario de los correos electrónicos en un formato de registro en su origen original para los administradores a fin de recuperarlos y validarlos.

- Se recomienda mantener la configuración a los valores predeterminados si decide habilitar el archivado de correos electrónicos. Los valores predeterminados son 10MB por registro y 10 registros máximo retenido. Los registros continuarán agregándose y reproduciéndose en función del tamaño del propio archivo de registro. Los archivos de registro de la caja de archivos se rellenan en función de la velocidad del tráfico de correo electrónico que pasa por el dispositivo. A medida que se crean más registros, se eliminan los registros de mbox de archivo más antiguos al espacio libre para la creación del nuevo registro.
- Asegúrese de que el dispositivo tenga suficiente espacio en disco antes de aumentar el tamaño de archivo de registro de mbox y el número máximo de archivos de registro retenidos.
- Para evitar que se generen los logs mbox de archivo, deberá inhabilitar la función de archivo por política.

Nota: El dispositivo de administración de seguridad (SMA) no puede recuperar los registros

de las casillas de archivo ESA y CES y se almacenan localmente para cada ESA y CES con la función activada.

¿Cómo se archivan los correos electrónicos en ESA y CES?

El archiving de correo electrónico está disponible con los filtros antispam, antivirus, protección frente a malware avanzado, graymail y mensajes. La acción de archivo se puede configurar mediante la interfaz gráfica de usuario (GUI) o la interfaz de línea de comandos (CLI) para antispam, antivirus, protección frente a malware avanzado y graymail.

En el caso de los filtros de mensajes, la acción de archivo se puede configurar sólo con la CLI.

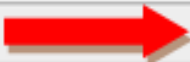
Configuración del archivo Anti-Spam

1. Vaya a la GUI > Políticas de correo > Políticas de correo entrante/saliente.
2. Haga clic en la configuración Anti-Spam para la política respectiva para configurar el archivado de correo electrónico.
3. Haga clic en **Avanzado** en la configuración disponible para Configuración de Spam Identificado Positivamente y/o Configuración de Spam Sospechoso.
4. Pulse el botón de opción situado junto a Sí para archivar correos electrónicos con el veredicto antispam correspondiente.
5. Envíe la configuración y realice estos cambios como se muestra en la imagen.

Positively-Identified Spam Settings	
Apply This Action to Message:	Spam Quarantine ▼ <i>Note: If local and external quarantines are defined, mail will be</i>
Add Text to Subject:	Prepend ▼ [SPAM]
▼ Advanced	
Add Custom Header (optional):	Header: <input type="text"/> Value: <input type="text"/>
Send to an Alternate Envelope Recipient (optional):	Email Address: <input type="text"/> <i>(e.g. employee@compa</i>
Archive Message:	<input checked="" type="radio"/> No <input type="radio"/> Yes

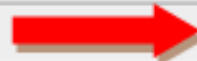
Configurar el archivo antivirus

1. Vaya a la GUI > Políticas de correo > Políticas de correo entrante/saliente.
2. Haga clic en la configuración del antivirus en la política respectiva para configurar el archivado del correo electrónico.
3. En cada uno de los veredictos de escaneo que desea archivar el mensaje original, pulse el botón de opción situado junto a Sí para archivar.
4. Envíe la configuración y realice estos cambios como se muestra en la imagen.

Repaired Messages:	
Action Applied to Message:	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
	[WARNING: VIRUS REMOVED]
▶ Advanced	Optional settings for custom header and message

Configuración del archivo de protección frente a malware avanzado

1. Vaya a la GUI > Políticas de correo > Políticas de correo entrante/saliente.
2. Haga clic en la configuración de protección frente a malware avanzado en la política respectiva para configurar el archiving de correo electrónico.
3. En cada uno de los veredictos de escaneo que desee para archivar el mensaje original, presione el botón de radio situado junto a Sí para archivar.
4. Envíe la configuración y realice estos cambios como se muestra en la imagen.

Messages with Malware Attachments:	
Action Applied to Message:	Drop Message ▼
 Archive Original Message:	<input type="radio"/> No <input checked="" type="radio"/> Yes
Drop Malware Attachments:	<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: MALWARE DETECTED]

Configurar el archivo de graymail

1. Vaya a la GUI > Políticas de correo > Políticas de correo entrante/saliente.
2. Haga clic en los parámetros de Graymail en la política respectiva para configurar el archivado del correo electrónico.
3. Haga clic en Avanzar en los parámetros disponibles para Marketing, Social y Bulk.
4. Pulse el botón de opción situado junto a Sí para archivar correos electrónicos con el veredicto correspondiente de Graymail.
5. Envíe la configuración y realice estos cambios.

Action on Marketing Email	
Apply this action to Message:	Deliver <input type="button" value="v"/> 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	Add Custom Header (optional): Header: <input type="text"/> Value: <input type="text"/>
	Send to an Alternate Envelope Recipient (optional): Email Address: <input type="text"/> (e.g. employee@)
	Archive Message: <input checked="" type="radio"/> No <input type="radio"/> Yes

Configurar archivo de filtro de mensajes

Nota: Se requiere un filtro de mensaje con acción de archivo para ver los registros archivados. Los filtros de mensajes sólo se pueden crear dentro de la CLI.

Filtro de ejemplo:

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

1. Inicie sesión en el dispositivo en la CLI.
2. Cree un filtro de mensaje como se ve en el filtro de ejemplo proporcionado.
3. Envíe este filtro y confirme los cambios.

Validar disponibilidad de registros Mbox de archivo

Cuando se confirma la configuración para el archivo para los servicios respectivos, los correos electrónicos archivados se almacenan en un archivo de registro con formato mbox. Para verificar si los registros de archivo están disponibles para la recuperación, navegue hasta la **GUI > Administración del sistema > Suscripciones de registro**.

Los archivos de servicios de seguridad crean un registro independiente con un tipo de registro de archivo como se muestra en 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 los filtros de mensajes, la configuración de archivo se ve **sólo** desde la CLI:

- **Filters > 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
```

Recuperar los registros de Mbox

Para dispositivos independientes, estos registros de mbox se pueden recuperar directamente desde la GUI. Navegue hasta **laGUI > Administración del sistema > Suscripciones de registro** y haga clic en **Archivos de registro** para el registro de archivo respectivo que recuperará.

Para los dispositivos en clúster, los registros de mbox se pueden recuperar con el uso de FTP/Secure Copy (SCP) como se describe en [este artículo](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 Cisco Email Security Appliance - Guías de usuario final](#)
- [¿Qué es el formato de buzón de correo UNIX?](#)
- [Dónde se almacenan los registros en el dispositivo de seguridad Cisco Email Security Appliance \(ESA\) y cómo puedo acceder a ellos](#)
- [Cómo extraer un correo electrónico de los registros de mbox de archivo](#)

- [Soporte Técnico y Documentación - Cisco Systems](#)