# Verificar las cargas del análisis del archivo en el ESA

## Contenido

[Introducción](#)
[Determine si las conexiones están cargadas para el análisis del archivo](#)
[Configure el AMP para el análisis del archivo](#)
[Revise los registros AMP para el análisis del archivo](#)
[Explicación de las etiquetas de la acción de la carga](#)
[“Situaciones de ejemplo”](#)
[Archivo cargado para el análisis](#)
[Archivo no cargado para el análisis porque el archivo se sabe ya](#)
[Carga del análisis del fichero de diario vía las encabezados del correo electrónico](#)
[Información Relacionada](#)

## Introducción

Este documento describe cómo determinar si los archivos que se procesan con la protección avanzada de Malware (AMP) en el dispositivo de seguridad del email de Cisco (ESA) están enviados para el análisis del archivo, y también qué el archivo del registro asociado AMP proporciona.

## Determine si las conexiones están cargadas para el análisis del archivo

Con el archivo se habilita el análisis, las conexiones que son analizadas por la reputación del archivo se pueden enviar para clasifiar el análisis para el análisis adicional. Esto proporciona el del más alto nivel de la protección contra el zero-day y las amenazas apuntadas. El análisis del archivo está solamente disponible cuando se habilita la filtración de la reputación del archivo.

Utilice las opciones de los tipos de archivo para limitar los tipos de archivos que se pudieron enviar a la nube. Los archivos específicos se envían que se basan siempre en las peticiones de la nube de los servicios del análisis del archivo, que apunta esos archivos para los cuales el análisis adicional sea necesario. El análisis del archivo para los tipos de archivo determinados pudo ser inhabilitado temporalmente en que el análisis del archivo mantiene la capacidad de los alcances de la nube.

> Nota: Refiera a los criterios del archivo para los servicios de protección avanzados de Malware para el documento de Cisco de los productos de seguridad del contenido de Cisco para el más actualizado y información adicional.

> Nota:  Revise por favor los Release Note y el guía del usuario para la revisión específica de AsyncOS que se ejecute en su dispositivo, como los tipos de archivo del análisis del archivo pueden variar basado en la versión de AsyncOS.

Tipos de archivo que pueden ser enviados para el análisis del archivo:

- Los tipos de archivo siguiente pueden ser enviados actualmente para el análisis: (Todas las versiones que soportan el análisis del archivo) executables de Windows, los archivos por ejemplo del .exe, del .dll, .sys, y .scr.Formato de documento portátil de Adobe (PDF), Microsoft Office 2007+ (XML abierto), Microsoft Office 97-2004 (OLE), Microsoft Windows/DOS ejecutable, otros tipos de archivo potencialmente malévolos.Las configuraciones de los tipos de archivo que usted ha seleccionado para la carga en el anti-Malware y de la reputación paginan (para la Seguridad de la red) o las configuraciones de la reputación y del análisis del archivo paginan (para la Seguridad del correo electrónico.) El soporte inicial incluye el PDF y Microsoft Office los archivos.(Principio en AsyncOS 9.7.1 para la Seguridad del correo electrónico) si usted ha seleccionado la otra opción potencialmente malévola de los tipos de archivo, Microsoft Office clasifía con las Extensiones siguientes guardadas en el formato XML o MHTML: ade, ADP, ADN, accdb, accdr, accdt, accda, mdb, BDC, mda, mdn, mdt, mdw, mdf, mde, accde, mam, maq, marcha, estera, maf, ldb, laccdb, doc., punto, docx, docm, dotx, dotm, docb, xls, xlt, xlm, xlsx, xlsm, xltx, xltm, xlsb, xla, xlam, xll, xlw, ppt, crisol, pps, pptx, pptm, potx, potm, ppam, ppsx, ppsm, sldx, sldm, mht, mhtm, mhtml, y xml.

  Nota: Si la carga en el servicio del análisis del archivo excede la capacidad, algunos archivos no pueden ser analizados incluso si seleccionan al tipo de archivo para el análisis y el archivo sería de otra manera elegible para el análisis. Usted recibirá una alerta cuando el servicio no puede temporalmente procesar los archivos de un tipo determinado.

Resaltar las NOTAS IMPORTANTES:

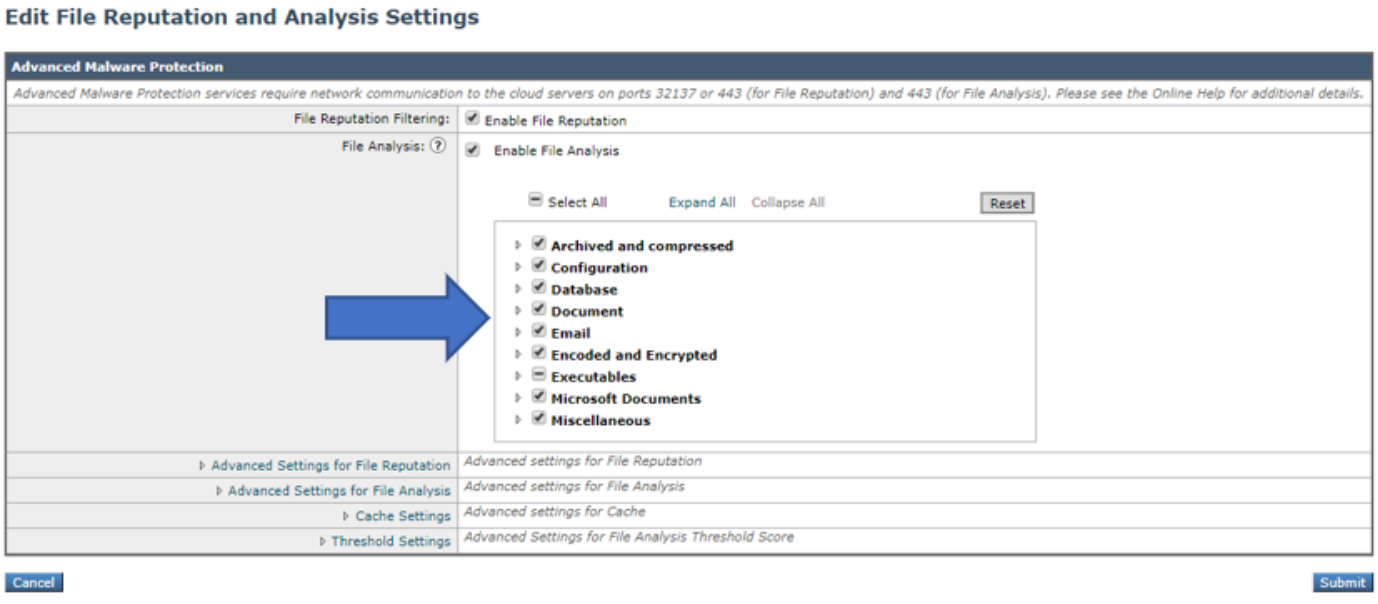
- Si un archivo ha estado cargado recientemente de cualquier fuente, el archivo no será cargado otra vez. Para los resultados del análisis del archivo para este archivo, búsqueda para el SHA-256 de la página de la información del análisis del archivo.
- El dispositivo intentará una vez cargar el archivo; si la carga no es acertada, por ejemplo debido a los problemas de conectividad, el archivo no puede ser cargado. Si era el error porque el servidor del análisis del archivo fue sobrecargado, la carga será intentada una vez más.

# Configuración AMP para el análisis del archivo

Por abandono, cuando un ESA primero se gira y tiene todavía establecer una conexión al updater de Cisco, el ÚNICO tipo de archivo del análisis del archivo enumerado será archivos ejecutables de “Microsoft Windows/DOS”.  Usted necesitará permitir que una actualización del servicio complete antes de ser permitida configurar los tipos de archivo adicionales.  Esto será reflejada en el archivo del registro de los updater_logs, visto como “fireamp.json”:

```
Sun Jul 9 13:52:28 2017 Info: amp beginning download of remote file
"http://updates.ironport.com/amp/1.0.11/fireamp.json/default/100116"
Sun Jul 9 13:52:28 2017 Info: amp successfully downloaded file
"amp/1.0.11/fireamp.json/default/100116"
Sun Jul 9 13:52:28 2017 Info: amp applying file "amp/1.0.11/fireamp.json/default/100116"
```

Para configurar el análisis del archivo vía el GUI, navegue a los **Servicios de seguridad > a la reputación del archivo y el análisis > edita las configuraciones globales…**




Para configurar el AMP para el análisis del archivo vía el CLI, ingrese el **ampconfig > el comando setup** y el movimiento a través del Asisitente de la respuesta. Usted debe seleccionar **Y** cuando le presentan con esta pregunta: **¿Usted quiere modificar los tipos de archivo para el análisis del archivo?**

```
myesa.local> ampconfig

File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
Adobe Portable Document Format (PDF)
Microsoft Office 2007+ (Open XML)
Microsoft Office 97-2004 (OLE)
Microsoft Windows / DOS Executable
Other potentially malicious file types
Appliance Group ID/Name: Not part of any group yet


Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- CLEARCACHE - Clears the local File Reputation cache.
[]> setup

File Reputation: Enabled
Would you like to use File Reputation? [Y]>

Would you like to use File Analysis? [Y]>

File types supported for File Analysis:

1. Archived and compressed [selected]
2. Configuration [selected]
3. Database [selected]
4. Document [selected]
5. Email [selected]
6. Encoded and Encrypted [selected]
7. Executables [partly selected]
8. Microsoft Documents [selected]
9. Miscellaneous [selected]
```

```
Do you want to modify the file types selected for File Analysis? [N]> y

Enter comma separated serial numbers from the "Supported" list. Enter "ALL" to select all
"currently" supported File Types.
[1,2,3,4,5]> ALL

Specify AMP processing timeout (in seconds)
[120]>

Advanced-Malware protection is now enabled on the system.
Please note: you must issue the 'policyconfig' command (CLI) or Mail
Policies (GUI) to configure advanced malware scanning behavior for
default and custom Incoming Mail Policies.
This is recommended for your DEFAULT policy.
```

De acuerdo con esta configuración, los tipos de archivo se habilitan que están conforme al análisis del archivo, como aplicable.

# Registros del estudio AMP para el análisis del archivo

Cuando las conexiones son analizadas por la reputación del archivo o clasifían el análisis en el ESA, se registran en el registro AMP. Para revisar este registro para todas las acciones AMP, funcione con la **cola amperio del** CLI ESA, o muévase a través del Asisitente de la respuesta para la **cola** o el **comando grep**. **El comando grep** es útil si usted conoce el archivo específico u otros detalles para los cuales usted desea de buscar en el registro AMP.

Aquí tiene un ejemplo:

```
mylocal.esa >  tail amp

Press Ctrl-C to stop.
Tue Aug 13 17:28:47 2019 Info: Compressed/Archive File: sha256 =
deace8ba729ad32313131321311232av2316623cfe9ac MID = 1683600, Extracted File: File Name =
'[redacted].pdf', File Type = 'application/pdf', sha256 =
deace8ba729ad32313131321311232av2316623cfe9ac, Disposition = LOWRISK, Response received from =
Cloud, Malware = None, Analysis Score = 0, upload_action = Recommended to send the file for
analysis
Thu Aug 15 13:49:14 2019 Debug: File reputation query initiating. File Name =
'amp_watchdog.txt', MID = 0, File Size = 12 bytes, File Type = text/plain
Thu Aug 15 13:49:14 2019 Debug: Response received for file reputation query from Cloud. File
Name = 'amp_watchdog.txt', MID = 0, Disposition = FILE UNKNOWN, Malware = None, Analysis Score =
0, sha256 = a5f28f1fed7c2fe88bcdf403710098977fa12c32d13bfbd78bbe27e95b245f82, upload_action =
Recommended not to send the file for analysis
```

> Nota: Las versiones anteriores de AsyncOS visualizarían “amp_watchdog.txt” en los registros AMP.  Éste es un archivo OS que se visualiza cada diez minutos en los registros. Este archivo es parte del señal de mantenimiento para el AMP y puede ser ignorado con seguridad.  Este archivo es el comenzar ocultado en AsyncOS 10.0.1 y más nuevo.

> Nota: Las versiones anteriores de AsyncOS registrarán la etiqueta del upload_action tienen tres valores que se define para que la carga clasifíe el comportamiento del análisis.

Las tres respuestas para la acción de la carga en un AsyncOS más viejo:

- “upload_action el = 0": El archivo se sabe al servicio de la reputación; no envíe para el

análisis.
- “upload_action el = 1": Envíe
- “upload_action el = 2": El archivo se sabe al servicio de la reputación; no envíe para el análisis

Las dos respuestas para la acción de la carga en la versión 12.x de AsyncOS y hacia adelante:

- el “upload_action = recomendó enviar el archivo para el análisis”
- **El debug registra solamente:** el “upload_action = recomendó no enviar el archivo para el análisis”

Esta respuesta dicta si un archivo está enviado para el análisis. Una vez más debe cumplir los criterios de los tipos de archivo configurados para ser sometido con éxito.

## Explicación de las etiquetas de la acción de la carga

```
"upload_action = 0": The file is known to the reputation service; do not send for analysis.
```

Para el "0," esto significa que el archivo “no está necesitado para ser enviado para la carga”. O, una mejor manera de mirarlo es, el archivo *se puede* enviar para que la carga clasifíe el análisis *si procede*.  Sin embargo, si el archivo entonces no se requiere el archivo no se envía.

```
"upload_action = 2": The file is known to the reputation service; do not send for analysis
```

Para el "2," que éste es un estricto “no envíe” el archivo para la carga.  Esta acción es final y decisiva, y se hace el proceso del análisis del archivo.

### “Situaciones de ejemplo”

Esta sección describe los escenarios posibles en los cuales los archivos están cargados para el análisis correctamente o no son cargado debido a una razón específica.

### Archivo cargado para el análisis

### Un AsyncOS más viejo:

Este ejemplo muestra un archivo DOCX que cumpla los criterios y se marque con etiqueta con el **upload_action = 1.** En la línea siguiente, el **archivo cargado para el** Secure Hash Algorithm (SHA) del **análisis** se registra al registro AMP también.

```
Thu Jan 29 08:32:18 2015 Info: File reputation query initiating. File Name = 'Lab_Guide.docx',
MID = 860, File Size = 39136 bytes, File Type = application/msword
Thu Jan 29 08:32:19 2015 Info: Response received for file reputation query from Cloud. File Name
= 'Royale_Raman_Lab_Setup_Guide_Beta.docx', MID = 860, Disposition = file unknown, Malware =
None, Reputation Score = 0, sha256 =
754e3e13b2348ffd9c701bd3d8ae96c5174bb8ebb76d8fb51c7f3d9567ff18ce, upload_action = 1
Thu Jan 29 08:32:21 2015 Info: File uploaded for analysis. SHA256:
754e3e13b2348ffd9c701bd3d8ae96c5174bb8ebb76d8fb51c7f3d9567ff18ce
```

### AsyncOS 12.x y hacia adelante:

Este ejemplo muestra un archivo PPTX que cumpla los criterios y se marque con etiqueta con el **upload_action = recomendado enviar el archivo para el análisis**. En la línea siguiente, el **archivo cargado para el** Secure Hash Algorithm (SHA) del **análisis** se registra al registro AMP también.

```
Thu Aug 15 09:42:19 2019 Info: Response received for file reputation query from Cloud. File Name
= 'ESA_AMP.pptx', MID = 1763042, Disposition = UNSCANNABLE, Malware = None, Analysis Score = 0,
sha256 = 0caade49103146813abaasd52edb63cf1c285b6a4bb6a2987c4e32, upload_action = Recommended to
send the file for analysis
Thu Aug 15 10:05:35 2019 Info: File uploaded for analysis. SHA256:
0caade49103146813abaasd52edb63cf1c285b6a4bb6a2987c4e32, file name: ESA_AMP.pptx
```

### Archivo no cargado para el análisis porque el archivo se sabe ya

### Un AsyncOS más viejo:

Este ejemplo muestra un archivo PDF que es analizado por el AMP con el **upload_action = 2** añadidos al final del fichero al registro de la reputación del archivo. Este archivo se sabe a la nube y no se requiere ya para ser cargado para el análisis, así que no está cargado otra vez.

```
Wed Jan 28 09:09:51 2015 Info: File reputation query initiating. File Name = 'Zombies.pdf', MID
= 856, File Size = 309500 bytes, File Type = application/pdf
Wed Jan 28 09:09:51 2015 Info: Response received for file reputation query from Cache. File Name
= 'Zombies.pdf', MID = 856, Disposition = malicious, Malware = W32.Zombies.NotAVirus, Reputation
Score = 7, sha256 = 00b32c3428362e39e4df2a0c3e0950947c147781fdd3d2ffd0bf5f96989bb002,
upload_action = 2
```

### AsyncOS 12.x y hacia adelante:

Este ejemplo muestra que el archivo de amp_watchdog.txt con el amperio abre una sesión el nivel de debug que corresponde con el **upload_action = recomendado no enviar el archivo para el análisis** añadido al final del fichero al registro de la reputación del archivo. Este archivo se sabe a la nube y no se requiere ya para ser cargado para el análisis, así que no está cargado otra vez.

```
Mon Jul 15 17:41:53 2019 Debug: Response received for file reputation query from Cache. File
Name = 'amp_watchdog.txt', MID = 0, Disposition = FILE UNKNOWN, Malware = None, Analysis Score =
0, sha256 = a5f28f1fed7c2fe88bcdf403710098977fa12c32d13bfbd78bbe27e95b245f82, upload_action =
Recommended not to send the file for analysis
```

## Carga del análisis del fichero de diario vía las encabezados del correo electrónico

Del CLI, con la opción usando el **logconfig del** comando, el submarino option de los **logheaders** se puede seleccionar para enumerar y para registrar las encabezados de los correos electrónicos procesados con el ESA.  Usando “X-Amperio-ARCHIVO-cargó” la encabezado, un archivo está cargado en cualquier momento o no cargado para el análisis del archivo será registrado a los registros del correo del ESA.

Mirando los registros del correo, resultados para los archivos cargados para el análisis:

```
Mon Sep 5 13:30:03 2016 Info: Message done DCID 0 MID 7659 to RID [0] [('X-Amp-File-Uploaded',
'True')]
```

Mirando los registros del correo, resultados para los archivos no cargados para el análisis:

```
Mon Sep 5 13:31:13 2016 Info: Message done DCID 0 MID 7660 to RID [0] [('X-Amp-File-Uploaded',
'False')]
```

# Información Relacionada

- Guías del usuario de AsyncOS
- Criterios del archivo para los servicios de protección avanzados de Malware para los productos de seguridad del contenido de Cisco
- Prueba avanzada de la protección ESA Malware (AMP)
- Soporte Técnico y Documentación - Cisco Systems