Verifying File Analysis Uploads on ESA

Contents

Introduction

This document describes how to determine whether files that are processed through Advanced Malware Protection (AMP) on the Cisco Email Security Appliance (ESA) are sent for file analysis, and also what the associated AMP log file provides.

Determine If Attachments Are Uploaded for File Analysis

With File Analysis is enabled, attachments that are scanned by File Reputation may be sent to File Analysis for further analysis. This provides the highest level of protection against zero-day and targeted threats. File Analysis is only available when File Reputation Filtering is enabled.

Use the File Types options in order to limit the types of files that might be sent to the Cloud. The specific files that are sent are always based on requests from the File Analysis services Cloud, which targets those files for which additional analysis is needed. File analysis for particular file types might be disabled temporarily when the File Analysis services Cloud reaches capacity.

> **Note**: Refer to the File Criteria for Advanced Malware Protection Services for Cisco Content Security Products Cisco document for the most up-to-date and additional information.

> **Note**: Please review the Release Notes and User Guide for the specific revision of AsyncOS that runs on your appliance, as the File Analysis file types may vary based on the version of AsyncOS.

File types that can be sent for file analysis:

- The following file types can currently be sent for analysis: (All releases that support File Analysis) Windows Executables, for example .exe, .dll, .sys, and .scr files.Adobe Portable Document Format (PDF), Microsoft Office 2007+ (Open XML), Microsoft Office 97-2004 (OLE), Microsoft Windows / DOS Executable, Other potentially malicious file types.File types

that you have selected for upload on the Anti-Malware and Reputation settings page (for Web Security) or the File Reputation and Analysis settings page (for Email Security.) Initial support includes PDF and Microsoft Office files.(Beginning in AsyncOS 9.7.1 for Email Security) If you have selected the Other potentially malicious file types option, Microsoft Office files with the following extensions saved in XML or MHTML format: ade, adp, adn, accdb, accdr, accdt, accda, mdb, cdb, mda, mdn, mdt, mdw, mdf, mde, accde, mam, maq, mar, mat, maf, ldb, laccdb, doc, dot, docx, docm, dotx, dotm, docb, xls, xlt, xlm, xlsx, xlsm, xltx, xltm, xlsb, xla, xlam, xll, xlw, ppt, pot, pps, pptx, pptm, potx, potm, ppam, ppsx, ppsm, sldx, sldm, mht, mhtm, mhtml, and xml.

Note: If the load on the File Analysis service exceeds capacity, some files may not be analyzed even if the file type is selected for analysis and the file would otherwise be eligible for analysis. You will receive an alert when the service is temporarily unable to process files of a particular type.

Highlighting important notes:

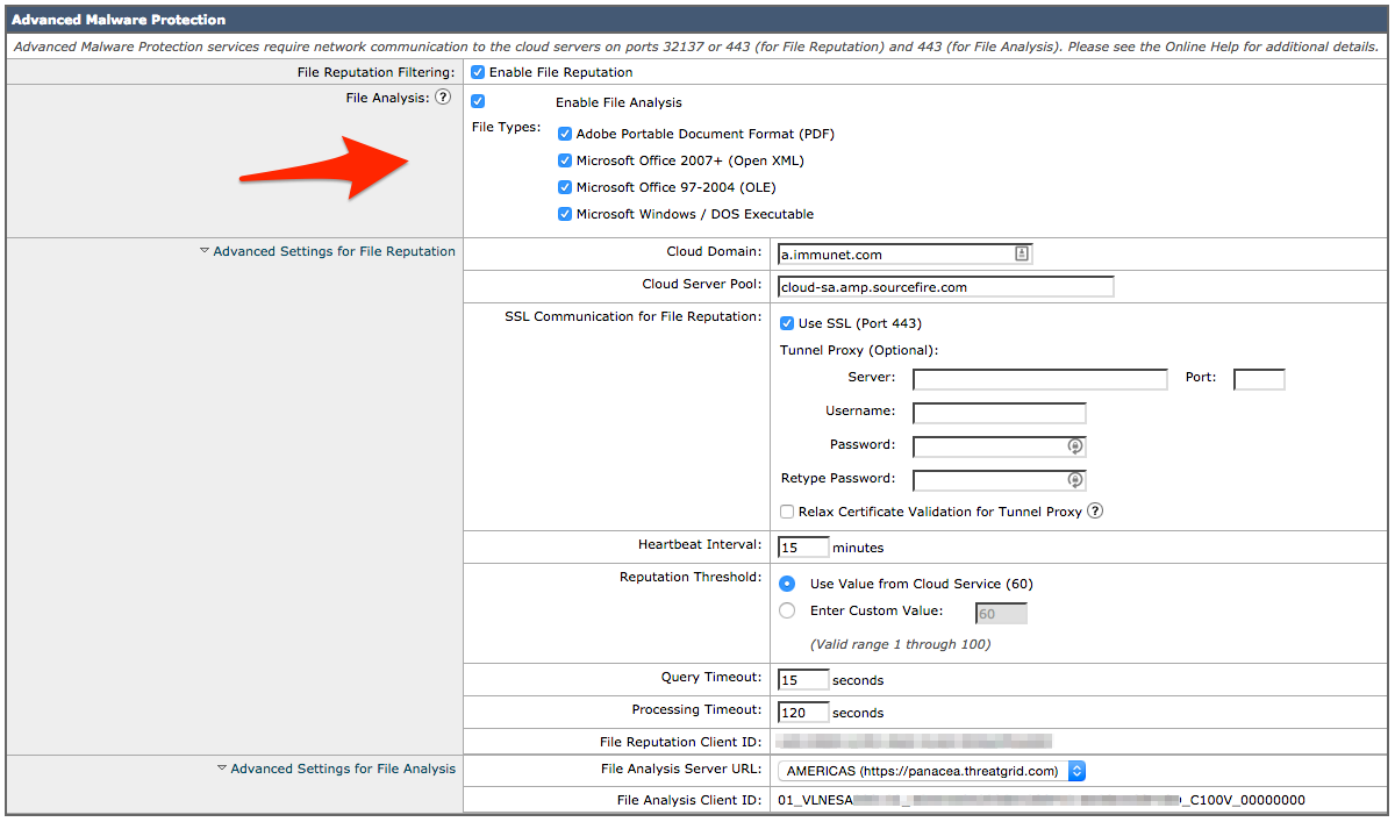
- If a file has recently been uploaded from any source, the file will not be uploaded again. For file analysis results for this file, search for the SHA-256 from the File Analysis reporting page.
- The appliance will try once to upload the file; if upload is not successful, for example because of connectivity problems, the file may not be uploaded. If the failure was because the file analysis server was overloaded, the upload will be attempted once more.

Configure AMP for File Analysis

By default, when an ESA is first turned on and has yet to establish a connection to the Cisco updater, the ONLY File Analysis file type listed will be "Microsoft Windows / DOS Executable" files. You will need to allow a service update to complete prior to being allowed to configure additional file types. This will be reflected in the updater_logs log file, seen as "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"
```

To configure File Analysis via the GUI, navigate to **Security Services > File Reputation and Analysis > Edit Global Settings...**



In order to configure AMP for File Analysis via the CLI, enter the **ampconfig > setup** command and move through the response wizard. You must select **Y** when you are presented with this question: **Do you want to modify the file types for File Analysis?**

```
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. Adobe Portable Document Format (PDF) [selected]
2. Microsoft Office 2007+ (Open XML) [selected]
3. Microsoft Office 97-2004 (OLE) [selected]
4. Microsoft Windows / DOS Executable [selected]
5. Other potentially malicious file types [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.
```

Based on this configuration, the file types that are enabled are subject to File Analysis, as applicable.

Review AMP Logs for File Analysis

When attachments are scanned by File Reputation or File Analysis on the ESA, they are recorded in the AMP log. In order to review this log for all AMP actions, run **tail amp** from the ESA's CLI, or move through the response wizard for either the **tail** or **grep** command. The **grep** command is useful if you know the specific file or other details for which you desire to search in the AMP log.

Here is an example:

```
myesa.local> tail amp

Press Ctrl-C to stop.
Mon Feb 2 14:45:35 2015 Info: File reputation query initiating. File Name = 'amp_watchdog.txt',
MID = 0, File Size = 12 bytes, File Type = text/plain
Mon Feb 2 14:45:35 2015 Info: Response received for file reputation query from Cache. File Name
= 'amp_watchdog.txt', MID = 0, Disposition = file unknown, Malware = None, Reputation Score = 0,
sha256 = a5f28f1fed7c2fe88bcdf403710098977fa12c32d13bfbd78bbe27e95b245f82, upload_action = 1
Mon Feb 2 14:55:35 2015 Info: File reputation query initiating. File Name = 'amp_watchdog.txt',
MID = 0, File Size = 12 bytes, File Type = text/plain
Mon Feb 2 14:55:35 2015 Info: Response received for file reputation query from Cache. File Name
= 'amp_watchdog.txt', MID = 0, Disposition = file unknown, Malware = None, Reputation Score = 0,
sha256 = a5f28f1fed7c2fe88bcdf403710098977fa12c32d13bfbd78bbe27e95b245f82, upload_action = 1
Mon Feb 2 15:05:35 2015 Info: File reputation query initiating. File Name = 'amp_watchdog.txt',
MID = 0, File Size = 12 bytes, File Type = text/plain
Mon Feb 2 15:05:35 2015 Info: Response received for file reputation query from Cache. File Name
= 'amp_watchdog.txt', MID = 0, Disposition = file unknown, Malware = None, Reputation Score = 0,
sha256 = a5f28f1fed7c2fe88bcdf403710098977fa12c32d13bfbd78bbe27e95b245f82, upload_action = 1
```

> **Note**: Older versions of AsyncOS would display "amp_watchdog.txt" in the AMP logs. This is an OS file that is displayed every ten minutes in the logs. This file is part of the keep-alive for AMP and may be safely ignored. This file is hidden starting in AsyncOS 10.0.1 and newer.

With the file(s) processed for reputation, they have the **upload_action** tagged at the end of the file reputation query. There are three responses for upload action:

- "upload_action = 0": The file is known to the reputation service; do not send for analysis.
- "upload_action = 1": Send
- "upload_action = 2": The file is known to the reputation service; do not send for analysis

This response dictates whether a file is sent for analysis. Again, it must meet the criteria of the configured file types in order to be successfully submitted.

Explanation of Upload Action "0" Versus Upload Action "2"

`"upload_action = 0": The file is known to the reputation service; do not send for analysis.`
For "0," this means that the file is "not needed to be sent for upload". Or, a better way to look at it is, the file *can* be sent for upload to File Analysis *if* required. However, if the file is *not* required then the file is not sent.

`"upload_action = 2": The file is known to the reputation service; do not send for analysis`
For "2," this is a strict "do not send" the file for upload. This action is final and decisive, and File Analysis processing is done.

Example Scenarios

This section describes possible scenarios in which files are either uploaded for analysis properly or are not uploaded due to a specific reason.

File Uploaded for Analysis

This example shows a DOCX file that meets the criteria and is tagged with the **upload_action = 1**. In the next line, the **File uploaded for analysis** Secure Hash Algorithm (SHA) is recorded to the AMP log as well.

```
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
```

File Not Uploaded for Analysis Because File Is Already Known

This example shows a PDF file that is scanned by AMP with the **upload_action = 2** appended to the file reputation log. This file is already known to the Cloud and is not required to be uploaded for analysis, so it is not uploaded again.

```
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
```

Logging File Analysis upload via email headers

From the CLI, with the option using the command **logconfig**, the sub-option of **logheaders** can be selected to list and log the headers of emails processed through the ESA. Using the "X-Amp-File-Uploaded" header, anytime a file is uploaded or not uploaded for file analysis will be recorded to the mail logs of the ESA.

Looking at the mail logs, results for files uploaded for analysis:

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

Looking at the mail logs, results for files not uploaded for analysis:

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

Related Information

- **AsyncOS User Guides**
- **File Criteria for Advanced Malware Protection Services for Cisco Content Security Products**
- **ESA Advanced Malware Protection (AMP) Test**
- **Technical Support & Documentation - Cisco Systems**