How to Submit a File in Threat Grid from the AMP for Endpoints Portal?

Contents

Introduction

This document describes the process to submit samples to the Threat Grid (TG) Cloud from the Advance Malware Protection (AMP) for Endpoints Portal.

Contributed by Yeraldin Sánchez, Cisco TAC Engineer.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco AMP for Endpoints
- TG Cloud

Components Used

The information in this document is based on Cisco AMP for Endpoints console version 5.4.20190709.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

These are the requirements for the scenario described in this document:

- Access to the Cisco AMP for Endpoints portal
- File size no more than 20MB
- Less than 100 submissions per day

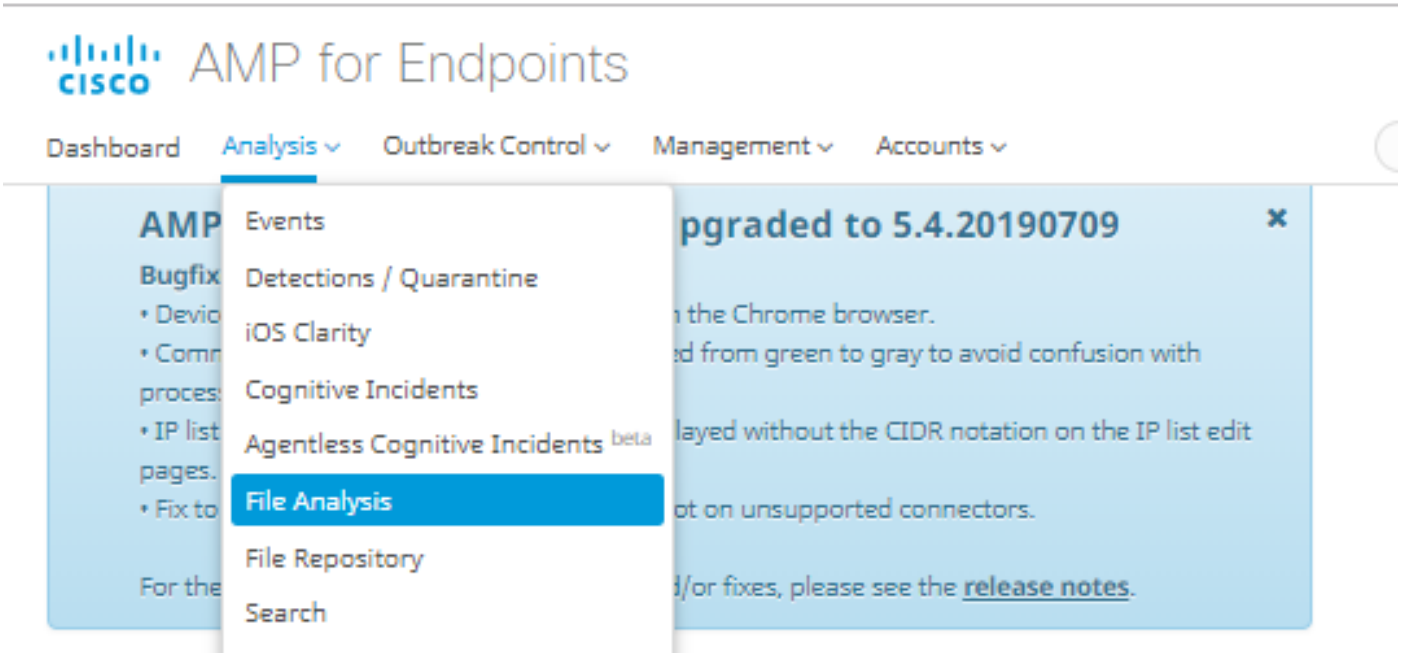
File Analysis limitations:

- File names are limited to 59 Unicode characters.
- Files may not be smaller than 16 bytes or larger than 20 MB
- Supported file types: **.exe, .dll, .jar, .swf, .pdf, .rtf, .doc(x), .xls(x), .ppt(x), .zip, .vbn and .sep**

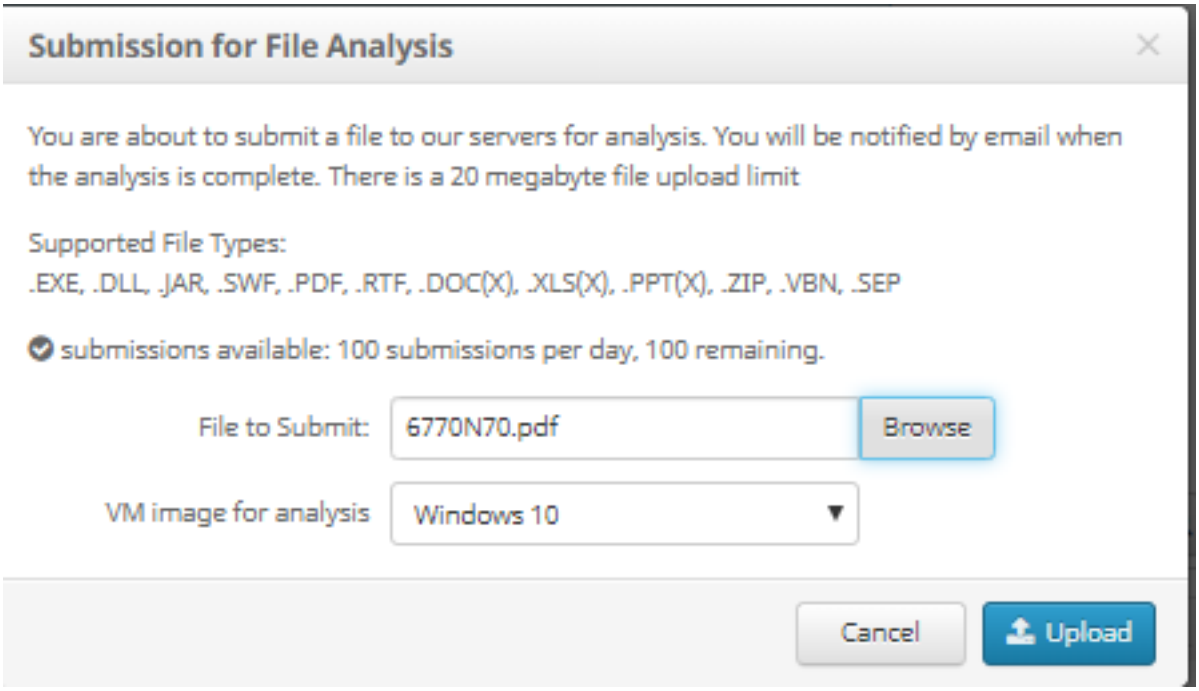
How to Submit a File in Threat Grid from the AMP for Endpoints Portal?

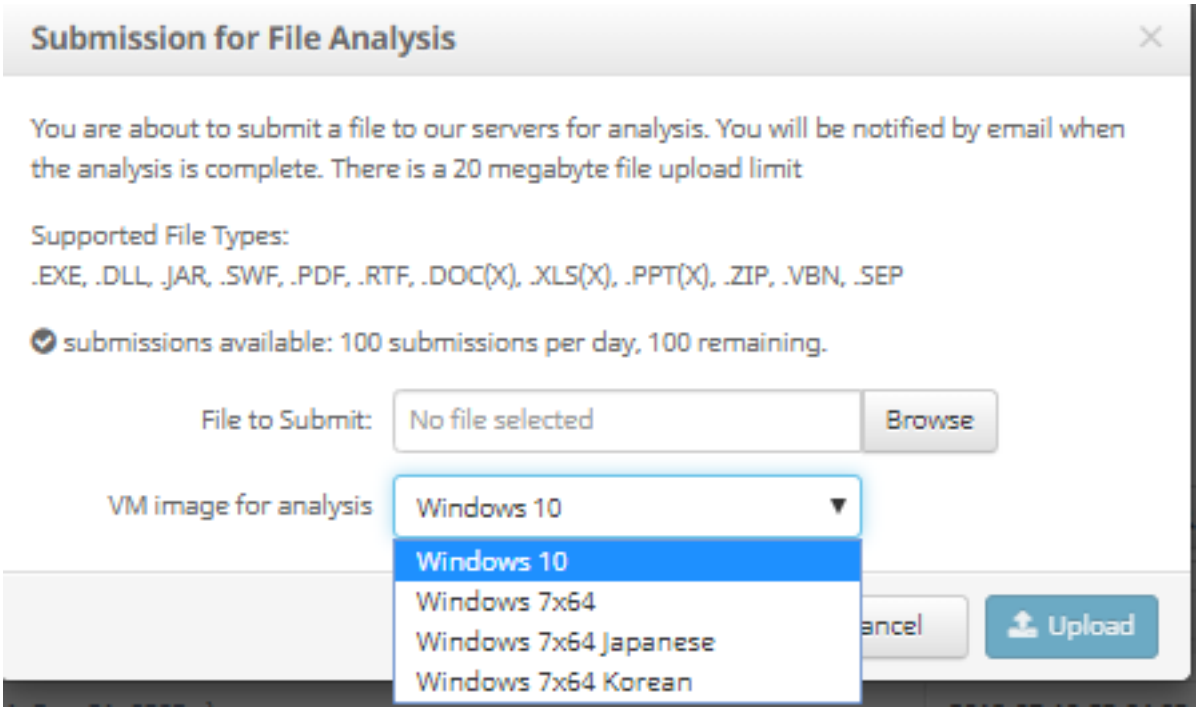
Here are the steps to follow in order to submit a sample to TG cloud from the AMP Portal.

Step 1. On the AMP portal, navigate to **Analysis > File Analysis**, as shown in the image.



Step 2. Select the file and Windows image version that you want to send for analysis, as shown in the images.

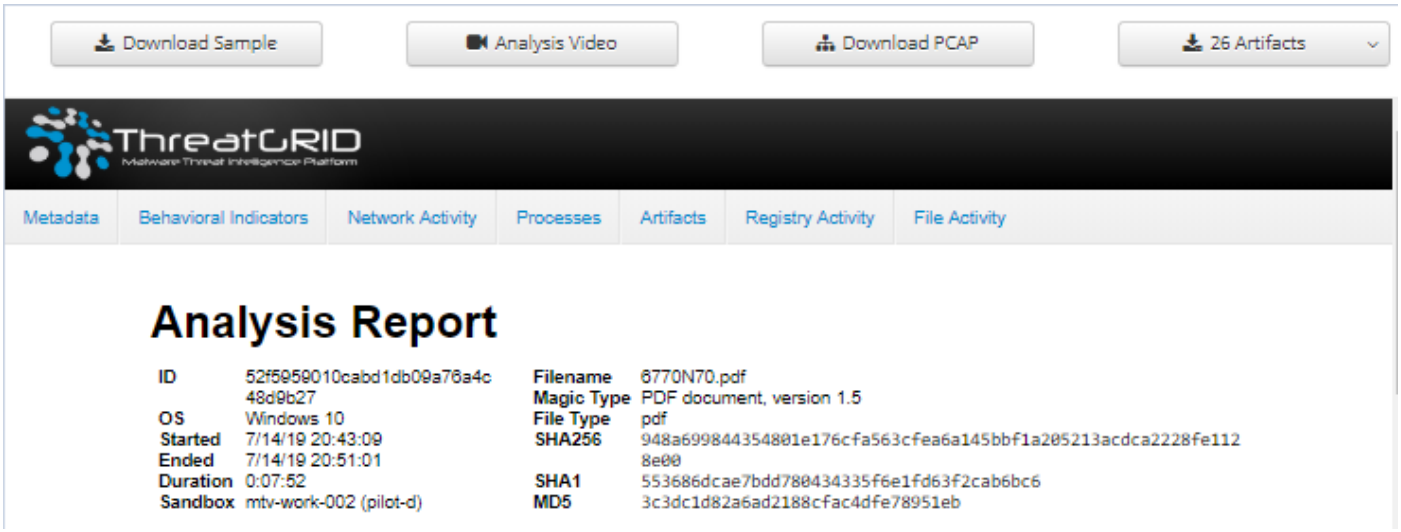




Step 3. Once the sample is uploaded, the analysis takes approximately 30 to 60 minutes to finish, it depends on system load, after this process is finished, an email notification is sent to your email.

Step 4. When the file analysis is ready, click on the **Report** button to have detailed information about the Threat Score obtained, as shown in the images.

6770N70.pdf (948a6998...e1128e00)		2019-07-14 20:43:04 UTC	Report 56
Fingerprint (SHA-256)	948a6998...e1128e00		
File name	6770N70.pdf		
Threat Score	56		
Behavioral Indicators	Name	Score	
	pdf-uri-action	56	
	pdf-contains-uris	25	



In order to have more information, you can find additional options for the file analysis:

Download Sample: This option allows you to download the sample.

Analysis Video: This option provides you the sample video obtained on the analysis.

Download PCAP: This option provides you a network connectivity analysis.

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

> **Warning**: Files downloaded from the File Analysis are often live malware and must be treated with extreme caution.

> **Note**: The analysis of a specific file is broken up into several sections. Some sections can not be available for all file types.

Related Information

- **Cisco AMP for Endpoints - User Guide**
- **Technical Support & Documentation - Cisco Systems**