Understand the Alert "Upload Limit Reached" on ESA with AMP

Contents

Introduction

This document describes the alert "Upload Limit Reached" the Email Security Appliance (ESA) throws when configured to scan emails with the Advanced Malware Protection (AMP) feature.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Email Security Appliance
- Advanced Malware Protection

Components Used

The information in this document is based on these software and hardware versions:

- Email Security Appliance (ESA) running software 12.x

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

The Email Security Appliance (ESA) uses the Advanced Malware Protection (AMP) feature which contains two main functions:

- File Reputation

- File Analysis

File Analysis uploads message attachments for sandbox analysis to ThreatGrid Cloud servers.

Understand the "Upload Limit Reached" Alert

Message Tracking can show emails were unscanned by Advanced Malware Protection (AMP) because they reached the upload limit.

Example:

```
02 Dec 2019 14:11:36 (GMT +01:00) Message 12345 is unscannable by Advanced Malware Protection engine. Reason: Upload Limit Reached
```

In the new ThreatGrid sample limits model, these limits are the number of samples that devices are allowed to upload for file analysis on per organization basis. All integrated devices (WSA, ESA, CES, FMC, etc.) as well as AMP for Endpoints are entitled to 200 samples per day, regardless of the number of devices.

This is a shared limit (not a limit per device), and this applies to licenses bought after 12/1/2017.

> **Note**: This counter is not reset every day, instead, this works as a 24 hours roll over period.

Example:

In a cluster of 4 ESAs with a 200 upload samples limit, if the ESA1 uploads 80 samples at 10:00 today, then, only 120 more samples can be uploaded among the 4 ESAs (shared limit) from today at 10:01 until tomorrow at 10:00, when the first 80 slots are released.

How can you Check the Number of Samples your ESAs have Uploaded in the past 24 Hours?

ESA: Navigate to **Monitor > AMP File Analysis** report and check the **Files Uploaded for Analysis** section.

SMA: Navigate to **Email > Reporting > AMP File Analysis** report and check the **Files Uploaded for Analysis** section.

> **Note**: If the AMP File Analysis report does not show accurate data, review the File Analysis Details in the Cloud Are Incomplete section in the User Guide.

> **Warning**: Refer to the defect CSCvm10813 for the additional information.

Alternatively, you can run a **grep** command from the CLI to count the number of files uploaded.

This must be done on each appliance.

Example:

```
grep "Dec 20.*File uploaded for analysis" amp -c
grep "Dec 21.*File uploaded for analysis" amp -c
```

You can use PCRE Regular Expressions to match the date and time.

How can you Extend the Upload Limit?

Contact your Account Manager or Sales Engineer within Cisco.

Related Information

- **Deep Dive into AMP and Threat Grid integration with Cisco Email Security**
- **Verifying File Analysis Uploads on ESA**
- **Technical Support & Documentation - Cisco Systems**