Troubleshoot Alert Message - Upload Limit Reached

Contents

Introduction

This document describes how to identify and resolve the **Upload Limit Reached** alert on the Email Security Appliance (ESA) when using Advanced Malware Protection (AMP).

Prerequisites

Requirements

Cisco recommends that you have basic knowledge of these topics:

- ESA
- AMP

Components Used

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

- ESA running AsyncOS 12.0 or newer

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

When the AMP feature is enabled on the ESA, it will perform one or both of the following main functions:

- File Reputation
- File Analysis

During File Analysis, specific attachments will be uploaded to ThreatGrid for sandboxing and analysis.

Understand the "Upload Limit Reached" Alert

Message Tracking can show emails not scanned by AMP because they have reached the upload limit.

Example

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

In the new ThreatGrid sample limits model, these limits are the number of samples devices can upload for File Analysis per organization. All integrated devices (WSA, ESA, CES, FMC, and so on) and AMP for Endpoints are collectively entitled to 200 samples daily, regardless of the number of devices.

Note: This counter is not reset daily; instead, it works as a 24-hour rollover period.

Example

In a cluster of 4 ESAs with a 200-sample upload limit, if 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 Cisco Bug ID CSCvm10813 for 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**