Troubleshoot "The File Reputation Service Is Not Reachable" Error on Cisco ESA

Contents

Introduction

Components Used

Prerequisites and Risks

Identify the Error

Validate File Reputation Settings

- From the GUI
- From the CLI

Verify Connectivity

- US and North America Region
- Canada Region
- Europe Region
- Australia Region
- APJC Region

Analyze AMP Logs

Register with Threat Grid

Related Information

Introduction

This document describes how to resolve the "File Reputation service is not reachable" alert on the Cisco Email Security Appliance (ESA).

Components Used

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.

Prerequisites and Risks

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

- Cisco Email Security Appliance AsyncOS 15.x or newer
- Advanced Malware Protection (AMP) licensed and enabled

Tip: Ensure that your firewall allows outbound communication on Port 443. If you use a tunnel

---

proxy, you can be required to enable the option to Relax Certificate Validation for Tunnel Proxy. This action skips standard certificate validation if the proxy server certificate is not signed by a root authority trusted by the ESA. For example, use this option if you use a self-signed certificate on a trusted internal tunnel proxy server.

Identify the Error

When AMP is licensed and enabled on the ESA, you receive this message:

```
<#root>

The Warning message is:

The File Reputation service is not reachable.

Last message occurred 2 times between Mon Feb 23 14:15:14 2026 and Mon Feb 23 14:16:23 2026.

Version: 15.5.1-055
Serial Number: 123A82F6780XXX9E1E10-XXX5DBEFCXXX
Timestamp: 23 Feb 2026 14:19:00 -0500
```

Validate File Reputation Settings

From the GUI

Ensure that the correct File Reputation server is selected. You can perform this in the GUI by navigating to **Security Services > File Reputation and Analysis > Edit Global Settings > Advanced Settings for File Reputation > File Reputation Server**. From there, select the Cloud appropriate to your region.

For hostname and port information to configure your firewall, review the Firewall Information section within the user guide.

From the CLI

Use the **ampconfig** command in the CLI to configure Advanced Malware Protection parameters. Use the **advanced** sub-command to set cloud query timeouts and select the reputation cloud.

```
<#root>

(Cluster example.com)>

ampconfig

File Reputation: Enabled
File Analysis: Enabled
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).
- SETGROUP - Add this appliance to the group of appliances that can share File Analysis reporting detai
- CACHESETTINGS - Configure the cache settings for AMP.
- CLUSTERSET - Set how advanced malware protection is configured in a cluster.
- CLUSTERSHOW - Display how advanced malware protection is configured in a cluster.
[]>
```

advanced

```
Enter cloud query timeout?
[20]>
```

Choose a file reputation server:

```
1. US Cloud
2. EU Cloud
3. APJC Cloud
4. Private reputation cloud
[1]>
```

Verify Connectivity

Review firewall and network settings to ensure that SSL communication is open for these ports for **File Reputation**:

US and North America Region

Purpose	Hostname	Default Port	Protocol	In / Out
File Reputation	cloud-esa-asn amp.cisco.com cloud-esa-est	443	TCP	Out.
File Analysis	panacea.threatgrid.com	443	TCP	Out

Canada Region

Purpose	Hostname	Default Port	Protocol	In / Out
File Analysis	panacea.threatgrid.ca	443	TCP	Out

Europe Region

Purpose	Hostname	Default Port	Protocol	In / Out
File Reputation	cloud-esa-asn eu.amp.cisco.com cloud-esa-est	443	TCP	Out.

File Analysis	panacea.threatgrid.eu	443	TCP	Out

Australia Region

Purpose	Hostname	Default Port	Protocol	In / Out
File Analysis	panacea.threatgrid.com.au	443	TCP	Out

APJC Region

Purpose	Hostname	Default Port	Protocol	In / Out
File Reputation	cloud-esa-asn apjc.amp.cisco.com cloud-esa-est	443	TCP	Out.
File Analysis	Can utilize Europe or North American hosts.	443	TCP	Out

To ensure the Email Security Appliance (ESA) can reach Cisco AMP services, verify connectivity over port 443 by using the following telnet commands from the CLI:

Connectivity Test Examples (US Region):

<#root>

```
(Machine esa.example.com)>
```

telnet amp.cisco.com 443

<#root>

```
(Machine esa.example.com)>
```

telnet panacea.threatgrid.com 443

Analyze AMP Logs

Review the current AMP log to determine service and connectivity status. Use the **tail amp** command in the CLI to observe real-time log entries.

If the File Reputation service is unreachable, the logs show these entries:

```
Mon Feb 23 10:11:16 2026 Warning: amp The File Reputation service in the cloud is unreachable.
Mon Feb 23 10:12:15 2026 Warning: amp The File Reputation service in the cloud is unreachable.
Mon Feb 23 10:13:15 2026 Warning: amp The File Reputation service in the cloud is unreachable.
```

After you correct the configuration in **ampconfig** > **advanced**, the logs show successful initialization:

```
Mon Feb 23 10:19:19 2026 Info: amp stunnel process started pid [3725]
Mon Feb 23 10:19:22 2026 Info: amp The File Reputation service in the cloud is reachable.
Mon Feb 23 10:19:22 2026 Info: amp File reputation service initialized successfully
Mon Feb 23 10:19:22 2026 Info: amp File Analysis service initialized successfully
Mon Feb 23 10:19:23 2026 Info: amp The File Analysis server is reachable
Mon Feb 23 10:20:24 2026 Info: amp File reputation query initiating. File Name =
'amp_watchdog.txt', MID = 0, File Size = 12 bytes, File Type = text/plain
Mon Feb 23 10:20:24 2026 Info: amp Response received for file reputation query
from Cloud. File Name = 'amp_watchdog.txt', MID = 0, Disposition = file unknown,
Malware = None, Reputation Score = 0, sha256 = a5f28f1fed7c2fe88bcdf403710098977
fa12c32d13bfbd78bbe27e95b245f82, upload_action = 1
```

The **amp_watchdog.txt** file runs every 10 minutes and is tracked in the AMP log. This file is part of the keep-alive for AMP. A normal query against a message with configured file types appears as follows:

```
Mon Feb 23 15:33:01 2026 Info: File reputation query initiating. File Name =
'securedoc_20260223T114401.html', MID = 703, File Size = 108769 bytes, File
Type = text/html
Mon Feb 23 15:33:02 2026 Info: Response received for file reputation query from
Cloud. File Name = 'securedoc_20260223T114401.html', MID = 703, Disposition = file
unknown, Malware = None, Reputation Score = 0, sha256 = c1afd8efe4eeb4e04551a8a0f5
533d80d4bec0205553465e997f9c672983346f, upload_action = 1
```

Register with Threat Grid

If the ESA can telnet to the file reputation server and no upstream proxy decrypts the connection, the appliance can require re-registration with Threat Grid. Use the hidden **ampregister** command within the **diagnostic** menu to initiate this process.

```
<#root>

esa.example.com>

diagnostic


Choose the operation you want to perform:
- RAID - Disk Verify Utility.
- DISK_USAGE - Check Disk Usage.
- NETWORK - Network Utilities.
- REPORTING - Reporting Utilities.
- TRACKING - Tracking Utilities.
- RELOAD - Reset configuration to the initial manufacturer values.
- SERVICES - Service Utilities.
[]>

ampregister


AMP registration initiated.
```

Related Information

- **ESA Advanced Malware Protection (AMP) Test**
- **ESA User Guides**
- **ESA FAQ: What is a Message ID (MID), Injection Connection ID (ICID), or Delivery Connection ID (DCID)?**
- **How do I search and view the mail logs on the ESA?**
- **Technical Support & Documentation - Cisco Systems**