Restart and View the Status of Service Engines Enabled on ESA/CES

Contents

[Introduction](#)

[Problem](#)

[Environment](#)

[Resolution](#)

[Related Information](#)

Introduction

This document describes how to restart and view the status of service engines on a Cisco Secure Email Gateway (ESA) or Cloud Email Security (CES).

Problem

Administrators can view or restart specific service engines (such as Anti-Spam, Anti-Virus, or DLP) on the appliance during troubleshooting. Starting in AsyncOS 11.1.x, users with administrative SSH access can perform these actions directly from the CLI.

Environment

- Cisco Secure Email Gateway (ESA)/CES
- AsyncOS version 11.1 or later
- Administrative Secure Shell (SSH) access

Resolution

⚠ **Caution**: Restarting service engines can temporarily impact mail flow or specific scanning capabilities. Services must only be restarted as part of troubleshooting specific known issues. If you are unsure of the impact, contact Cisco TAC before you proceed.

---

1. Connect to the appliance via SSH and run the **diagnostic** command, then choose **services**.

```
lab.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.
[]> services
```

2. Choose the service you want to manage (for example, **antispam**).

```
Choose one of the following services:
- ANTISPAM - Anti-Spam services
- ANTIVIRUS - Anti-Virus services
- DLP - Cisco Data Loss Prevention services
- ENCRYPTION - Encryption services
- GRAYMAIL - Graymail services
- REPORTING - Reporting associated services
- TRACKING - Tracking associated services
- EUQWEB - End User Quarantine GUI
- WEBUI - Web GUI
- SMART_LICENSE - Smart Licensing Agent
- ETF - External Threat Feeds
- SDR - Sender Domain Reputation
- IP_REP_CLIENT - Sender IP Reputation Client
- URL_REPUTATION_CLIENT - URL Reputation Client
- SERVICE_LOG_CLIENT - Service Log Client
[]> antispam
```

3. Choose the specific scanner if prompted (for example, **case**).

```
Choose one of the following type of scanners:
- CASE - CASE
- IMS - Intelligent Multi Scan
[]> case
```

4. View the current status of the service.

```
Choose the operation you want to perform:
- RESTART - Restart the service
- STATUS - View status of the service
[]> status

CASE has been up for 38m 38s.
```

5. Restart the service.

```
Choose one of the following type of scanners:
- CASE - CASE
- IMS - Intelligent Multi Scan
[]> case

Choose the operation you want to perform:
- RESTART - Restart the service
- STATUS - View status of the service
[]> restart

Restart command processed. The service CASE should be up in a moment.
```

6. (Validation) Verify that the service has restarted successfully by checking the status again. The uptime must reset.

```
Choose one of the following type of scanners:
- CASE - CASE
- IMS - Intelligent Multi Scan
[]> case

Choose the operation you want to perform:
- RESTART - Restart the service
- STATUS - View status of the service
[]> status

CASE has been up for 13s.
```

Related Information

- Cisco AsyncOS 11.1 for Cisco Email Security Appliances Release Notes
- Cisco Email Security Appliance End-User Guides
- Cisco Email Security Appliance Release Notes and General Information
- Product Technical Support and Documentation