

# CISCO Secure Email Gateway Integrations

The **Cisco Email Security Appliance (ESA)** integration is a comprehensive solution for managing and securing email traffic within an organization's network. It provides various functionalities, such as **spam filtering**, **virus scanning**, **policy enforcement**, and **data loss prevention**. The integration collects and parses data from the **Cisco Secure Email Gateway** (formerly known as **Cisco Email Security Appliance**) to provide valuable insights into the email environment. The data collection occurs through multiple methods, primarily through **TCP/UDP communication** and **log file analysis**.

---

## Requirements:

- Cisco account
  - Elastic agent already installed
- 

## Compatibility

This module has been tested against **Cisco Secure Email Gateway server version 14.0.0 Virtual Gateway C100V with the below given logs pattern**.

---

## Setup

### Configurations

- Sign-in to Cisco Secure Email Gateway Portal and follow the below steps for configurations:
  1. In Cisco Secure Email Gateway Administrator Portal, go to **System Administration** > **Log Subscriptions**.
  2. Click **Add Log Subscription**.
  3. Enter all the **Required Details**.
  4. Set **Log Name** as below for the respective category:
    - AMP Engine Logs -> amp
    - Anti-Spam Logs -> antispam
    - Antivirus Logs -> antivirus
    - Authentication Logs -> authentication

- Bounce Logs -> bounces
  - Consolidated Event Logs -> consolidated\_event
  - Content Scanner Logs -> content\_scanner
  - HTTP Logs -> gui\_logs
  - IronPort Text Mail Logs -> error\_logs
  - Text Mail Logs -> mail\_logs
  - Status Logs -> status
  - System Logs -> system
5. Select **Log Level** as Information.
  6. Select **Retrieval Method**.
  7. Click **Submit** and commit the Changes.

## Note

- **Retrieval Method** Supported:
  - **FTP Push to Remote Server** for the below categories: AMP Engine Logs, Anti-Spam Logs, Antivirus Logs, Authentication Logs, Bounce Logs, Consolidated Event Logs, Content Scanner Logs, HTTP Logs, IronPort Text Mail Logs, Text Mail Logs, Status Logs and System Logs.
  - **Syslog Push** for the below categories: AMP Engine Logs, Anti-Spam Logs, Antivirus Logs, Consolidated Event Logs, Content Scanner Logs, HTTP Logs, IronPort Text Mail Logs, Text Mail Logs, Status Logs and System Logs.

*If you need further assistance, kindly contact our support at [support@cytechint.com](mailto:support@cytechint.com) for prompt assistance and guidance.*

---

Revision #2

Created 3 December 2024 05:18:14 by David Napoleon Romanillos

Updated 3 December 2024 05:35:37 by David Napoleon Romanillos