# Securing Email with Cisco Email Security Appliance (SESAv3.2) Course

**Course Duration: 32 Hours** **Course Code: SESAv3.2**

## 1. Course Overview

The *Securing Email with Cisco Email Security Appliance (SESAv3.2)* course provides in-depth knowledge and hands-on experience to secure and manage email communication using Cisco's industry-leading email security solutions. Participants will learn how to deploy, configure, operate, and troubleshoot Cisco ESA to protect against phishing, spam, malware, and data loss while ensuring secure business communication.

## 2. What You'll Learn?

By the end of this course, you will be able to:

- Understand the features, capabilities, and architecture of Cisco ESA.
- Configure and manage security policies to protect email traffic.
- Implement advanced threat defense against spam, phishing, and malware.
- Configure data loss prevention (DLP) and encryption features.
- Monitor, analyze, and troubleshoot Cisco ESA operations.
- Integrate ESA with other Cisco security solutions.

## 3. Target Audience

This course is designed for:

- Network Security Engineers
- Email Security Administrators
- IT Security Specialists
- System Administrators
- Technical Support Personnel responsible for email security solutions

## 4. Pre-Requisites

To make the most of this training, participants should have:

- Basic knowledge of TCP/IP and networking concepts
- Familiarity with email protocols (SMTP, POP3, IMAP)
- General understanding of security concepts and firewall operations
- Experience with Cisco security products is recommended but not mandatory

## 5. Course Content

**Module 1: Introduction to Cisco Email Security Appliance**

- ESA features and benefits
- Deployment options and architecture
- Basic setup and initial configuration

**Module 2: Email Security Policies and Filtering**

- Anti-spam and anti-virus filtering
- Policy configuration and application
- Content and attachment filtering

**Module 3: Advanced Threat Defense**

- Phishing and spoofing protection

- Reputation and blacklisting services
- Advanced malware protection (AMP) integration

**Module 4: Data Security and Encryption**

- Data loss prevention (DLP) configuration
- Email encryption methods
- Policy-based encryption deployment

**Module 5: System Administration and Monitoring**

- Logging and reporting
- Monitoring email traffic and performance
- Troubleshooting common issues

**Module 6: ESA Integration and Best Practices**

- Integration with Cisco Security ecosystem
- High availability and redundancy
- Security best practices for email protection



**Phone:** +91-999-911-1686 **Mail Us:** info@ssdntech.com