# Securing Email with Cisco Email Security Appliance (SESA) V3.2

## Securing Email with Cisco Email Security Appliance (SESA) V3.2

The Securing Email with Cisco Email Security Appliance (SESA) training shows you how to deploy and use Cisco® Email Security Appliance to establish protection for your email systems against phishing, business email compromise, and ransomware, and to help streamline email security policy management. This hands-on training provides you with the knowledge and skills to implement, troubleshoot, and administer Cisco Email Security Appliance, including key capabilities, such as advanced malware protection, spam blocking, anti-virus protection, outbreak filtering, encryption, quarantines, and data loss prevention.

This training prepares you for the 300-720 SESA v1.1 exam. If passed, you earn the Cisco Certified Specialist – Email Content Security certification and satisfy the concentration exam requirement for the CCNP Security certification. This training also earns you 24 Continuing Education (CE) credits towards recertification.

### How you'll benefit

This class will help you:

- Deploy high-availability email protection against the dynamic, rapidly changing threats affecting your organization
- Gain leading-edge career skills focused on enterprise security
- Prepare for the 300-720 SESA v1.1 exam
- Earn 24 CE credits toward recertification

### Why Attend with Current Technologies CLC

- Our Instructors are in the top 10% rated by Cisco
- Our Lab has a dedicated 1 Gig Fiber Connection for our Labs
- Our Labs run up to Date Code for all our courses

### Who Should Attend

The primary audience for this course is as follows:

- Security Engineer
- Security Administrators
- Security Architects
- Operations Engineers
- Network Engineer
- Network Administrator
- Network or Security Technicians
- Network Manager
- Systems Designers
- Cisco Integrators and Partners

**Course Duration**
4 days

**Course Price**
$3,595.00 or 36 CLCs

**Methods of Delivery**
- Instructor Led
- Virtual ILT
- On-Site

**OUTLINE**

**Module 1: Describing the Cisco Email Security Appliance**

- Cisco Email Security Appliance Overview
- Technology Use Case
- Cisco Email Security Appliance Data Sheet
- SMTP Overview
- Email Pipeline Overview
- Installation Scenarios
- Initial Cisco Email Security Appliance Configuration
- Centralizing Services on a Cisco Content Security Management Appliance (SMA)
- Release Notes for AsyncOS 11.x

**Module 2: Controlling Sender and Recipient Domains**

- Public and Private Listeners
- Configuring the Gateway to Receive Email
- Host Access Table Overview
- Recipient Access Table Overview
- Configuring Routing and Delivery Features

**Module 3: Controlling Spam with Talos SenderBase and Anti-Spam**

- SenderBase Overview
- Anti-Spam
- Managing Graymail
- Protecting Against Malicious or Undesirable URLs
- File Reputation Filtering and File Analysis
- Bounce Verification

**Module 4: Using Anti-Virus and Outbreak Filters**

- Anti-Virus Scanning Overview
- Sophos Anti-Virus Filtering
- McAfee Anti-Virus Filtering
- Configuring the Appliance to Scan for Viruses
- Outbreak Filters
- How the Outbreak Filters Feature Works
- Managing Outbreak Filters

**Module 5: Using Mail Policies**

- Email Security Manager Overview
- Mail Policies Overview
- Handling Incoming and Outgoing Messages Differently
- Matching Users to a Mail Policy
- Message Splintering
- Configuring Mail Policies

**Module 6: Using Content Filters**

- Content Filters Overview
- Content Filter Conditions
- Content Filter Actions
- Filter Messages Based on Content
- Text Resources Overview
- Using and Testing the Content Dictionaries Filter Rules
- Understanding Text Resources
- Text Resource Management
- Using Text Resources

**Module 7: Using Message Filters**

- Message Filters Overview
- Components of a Message Filter
- Message Filter Processing
- Message Filter Rules
- Message Filter Actions
- Attachment Scanning
- Examples of Attachment Scanning Message Filters
- Using the CLI to Manage Message Filters
- Message Filter Examples
- Configuring Scan Behavior

**Module 8: Preventing Data Loss**

- Overview of the Data Loss Prevention (DLP) Scanning Process
- Setting Up Data Loss Prevention
- Policies for Data Loss Prevention
- Message Actions
- Updating the DLP Engine and Content Matching Classifiers

**Module 9: Using LDAP**

- Overview of LDAP
- Working with LDAP
- Using LDAP Queries
- Authenticating End-Users of the Spam Quarantine
- Configuring External LDAP Authentication for Users
- Testing Servers and Queries
- Using LDAP for Directory Harvest Attack Prevention
- Spam Quarantine Alias Consolidation Queries
- Validating Recipients Using an SMTP Server

**Module 10: SMTP Session Authentication**

- Configuring AsyncOS for SMTP Authentication
- Authenticating SMTP Sessions Using Client Certificates
- Checking the Validity of a Client Certificate
- Authenticating User Using LDAP Directory
- Authenticating SMTP Connection Over Transport Layer Security (TLS) Using a Client Certificate
- Establishing a TLS Connection from the Appliance
- Updating a List of Revoked Certificates

**Module 11: Using Email Authentication**

- Email Authentication Overview
- Configuring DomainKeys and DomainKeys Identified Mail (DKIM) Signing
- Verifying Incoming Messages Using DKIM
- Overview of Sender Policy Framework (SPF) and SIDF Verification
- Domain-based Message Authentication Reporting and Conformance (DMARC) Verification
- Forged Email Detection

**Module 12: Using Email Encryption**

- Overview of Cisco Email Encryption
- Encrypting Messages
- Determining Which Messages to Encrypt
- Inserting Encryption Headers into Messages
- Encrypting Communication with Other Message Transfer Agents (MTAs)
- Working with Certificates

- Managing Lists of Certificate Authorities
- Enabling TLS on a Listener's Host Access Table (HAT)
- Enabling TLS and Certificate Verification on Delivery
- Secure/Multipurpose Internet Mail Extensions (S/MIME) Security Services

**Module 13: Administering the Cisco Email Security Appliance**

**Module 14: Using System Quarantines and Delivery Methods**

- Describing Quarantines
- Spam Quarantine
- Setting Up the Centralized Spam Quarantine
- Using Safelists and Blocklists to Control Email Delivery Based on Sender
- Configuring Spam Management Features for End Users
- Managing Messages in the Spam Quarantine
- Policy, Virus, and Outbreak Quarantines
- Managing Policy, Virus, and Outbreak Quarantines
- Working with Messages in Policy, Virus, or Outbreak Quarantines
- Delivery Methods

**Module 15: Centralized Management Using Clusters**

- Overview of Centralized Management Using Clusters
- Cluster Organization
- Creating and Joining a Cluster
- Managing Clusters
- Cluster Communication
- Loading a Configuration in Clustered Appliances
- Best Practices

**Module 16: Testing and Troubleshooting**

- Debugging Mail Flow Using Test Messages: Trace
- Using the Listener to Test the Appliance
- Troubleshooting the Network
- Troubleshooting the Listener
- Troubleshooting Email Delivery
- Troubleshooting Performance
- Web Interface Appearance and Rendering Issues
- Responding to Alerts
- Troubleshooting Hardware Issues
- Working with Technical Support

**LAB OUTLINE**

- **Lab 1: Verify and Test Cisco ESA Configuration**
- **Lab 2: Advanced Malware in Attachments (Macro Detection)**
- **Lab 3: Protect Against Malicious or Undesirable URLs Beneath Shortened URLs**
- **Lab 4: Protect Against Malicious or Undesirable URLs Inside Attachments**
- **Lab 5: Intelligently Handle Unscannable Messages**
- **Lab 6: Leverage AMP Cloud Intelligence Via Pre-Classification Enhancement**

- **Lab 7: Integrate Cisco ESA with AMP Console**
- **Lab 8: Prevent Threats with Anti-Virus Protection**
- **Lab 9: Applying Outbreak Filters**
- **Lab 10: Configure Attachment Scanning**
- **Lab 11: Configure Outbound Data Loss Prevention**
- **Lab 12: Integrate Cisco ESA with LDAP and Enable the LDAP Accept Query**
- **Lab 13: Domain Keys Identified Mail (DKIM)**
- **Lab 14: Sender Policy Framework (SPF)**
- **Lab 15: Forged Email Detection**
- **Lab 16: Perform Basic Administration**
- **Lab 17: Configure the Cisco SMA for Tracking and Reporting**