# SESA - SECURING EMAIL WITH CISCO EMAIL SECURITY APPLIANCE V3.2

Course Code: 100499

This course helps you prepare to take the exam, Securing Email with Cisco Email Security Appliance (300-720 SESA), which leads to CCNP Security and the Certified Specialist - Email Content Security certifications. Learn to deploy high-availability email protection against the dynamic, rapidly changing threats affecting your organization as well as Gain leading-edge career skills focused on enterprise security.

Learn how to deploy and use Cisco® Email Security Appliance to establish protection for your email systems against phishing, business email compromise and ransomware. Help streamline email security policy management. This hands-on course 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 course is worth 24 Continuing Education (CE) Credits.**

## What You'll Learn

After completing this course, you should be able to:

- Describe and administer the Cisco Email Security Appliance (ESA)
- Control sender and recipient domains
- Control spam with Talos SenderBase and anti-spam
- Use anti-virus and outbreak filters
- Use mail policies
- Use content filters
- Use message filters
- Prevent data loss
- Perform LDAP queries
- Authenticate Simple Mail Transfer Protocol (SMTP) sessions
- Authenticate email
- Encrypt email
- Use system quarantines and delivery methods
- Perform centralized management using clusters
- Test and troubleshoot

## Who Needs to Attend

Individuals responsible for the deployment, administration and troubleshooting of a Cisco Email Security Appliance.

## Prerequisites

**Attendees should meet the following prerequisites:**

- TCP/IP services, including Domain Name System (DNS), Secure Shell (SSH), FTP, Simple Network Management Protocol (SNMP), HTTP, and HTTPS
- Experience with IP routing

**It is recommended that you have one of the following:**

- Cisco certification (Cisco CCNA® certification or higher)
- Relevant industry certification, such as (ISC)2, CompTIA Security+, EC-Council, Global Information Assurance Certification (GIAC), and ISACA
- Cisco Networking Academy letter of completion (CCNA® 1 and CCNA 2)
- Windows expertise: Microsoft [Microsoft Specialist, Microsoft Certified Solutions Associate (MCSA), Microsoft Certified Systems Engineer (MCSE)], CompTIA (A+, Network+, Server+)

# SESA - SECURING EMAIL WITH CISCO EMAIL SECURITY APPLIANCE V3.2

Course Code: 100499

| | | |
|---|---|---|
| VIRTUAL CLASSROOM LIVE | $3,595 USD | 4 Day |

## Virtual Classroom Live Outline

### 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

### 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

### 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

### 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

**Using Mail Policies**

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

**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

**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

**Preventing Data Loss**

- 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

**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

**Describing 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

**Using Email Authentication**

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

**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

**Administering the Cisco Email Security Appliance**

- Distributing Administrative Tasks
- System Administration
- Managing and Monitoring Using the Command Line Interface (CLI)
- Other Tasks in the GUI
- Advanced Network Configuration
- Using Email Security Monitor

- Tracking Messages
- Logging

### 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

### 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

### 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

## Virtual Classroom Live Labs

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

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

Sep 2 - 5, 2025 | 8:30 AM - 4:30 PM EDT

# SESA - SECURING EMAIL WITH CISCO EMAIL SECURITY APPLIANCE V3.2

Course Code: 100499

| | |
|---|---|
| ON-DEMAND | $800 USD |

## On-Demand Outline

**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

**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

**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

**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

**Using Mail Policies**

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

**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

**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

**Preventing Data Loss**

- 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

**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

**Describing 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

**Using Email Authentication**

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

**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

**Administering the Cisco Email Security Appliance**

- Distributing Administrative Tasks
- System Administration
- Managing and Monitoring Using the Command Line Interface (CLI)
- Other Tasks in the GUI
- Advanced Network Configuration
- Using Email Security Monitor

- Tracking Messages
- Logging

### 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

### 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

### 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

## On-Demand Labs

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

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

Visit us at www.globalknowledge.com or call us at 1-866-716-6688.

Date created: 4/19/2025 10:55:29 AM