

Dieses Training zeigt Ihnen, wie Sie die Cisco® Email Security Appliance einsetzen und verwenden, um Ihre E-Mail-Systeme vor Phishing, E-Mail-Kompromittierungen und Ransomware zu schützen und die Verwaltung von E-Mail-Sicherheitsrichtlinien zu optimieren.

Dieser praxisorientierte Kurs vermittelt Ihnen die Kenntnisse und Fähigkeiten zur Implementierung, Fehlerbehebung und Verwaltung der Cisco Email Security Appliance, einschließlich wichtiger Funktionen wie erweiterter Malware-Schutz, Spam-Blockierung, Virenschutz, Filterung von Ausbrüchen, Verschlüsselung, Quarantänen und Verhinderung von Datenverlusten.

### Kursinhalt

- 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 to enforce email policies
- 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

**E-Book** Sie erhalten die englischen Original-Unterlagen als Cisco E-Book. Bei der Cisco Digital Learning Version sind die Inhalte der Kursunterlage stattdessen in die Lernoberfläche integriert.

### Zielgruppe

- Security Engineers
- Security Administratoren
- Security Architekten
- Operations Engineers
- Network Engineers
- Network Administratoren
- Network oder Security Techniker
- Network Managers
- System Designers
- Cisco Integratoren und Partner

### Voraussetzungen

Sie sollten Sie über eine oder mehrere der folgenden technischen Grundkenntnisse verfügen:

- Cisco-Zertifizierung (Cisco CCENT®-Zertifizierung oder höher)
- Relevante Branchenzertifizierungen wie (ISC)2, CompTIA Security+, EC-Council, Global Information Assurance Certification (GIAC) und ISACA
- Abschluss der Cisco Networking Academy (CCNA® 1 und CCNA® 2)
- Windows-Know-how: Microsoft (Microsoft Specialist, Microsoft Certified Solutions Associate (MCSA), Microsoft Certified Systems Engineer (MCSE), CompTIA (A+, Network+, Server+)

Zudem folgende Kenntnisse und Fähigkeiten:

TCP/IP-Dienste, einschließlich Domain Name System (DNS), Secure Shell (SSH), FTP, Simple Network Management Protocol (SNMP), HTTP und HTTPS; Erfahrung mit IP-Routing.

### Kursziel

Dieser Kurs bereitet Sie auf die Prüfung Securing Email with Cisco Email Security Appliance innerhalb der CCNP® Security Zertifizierung vor und zudem auf den Certified Specialist – Email Content Security.

### Bearbeitungszeit

ca. 24 Stunden

### Dieser Kurs im Web



Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: [www.experteach.de/go/SESA](http://www.experteach.de/go/SESA)

### Vormerkung

Sie können auf unserer Website einen Platz kostenlos und unverbindlich für 7 Tage reservieren. Dies geht auch telefonisch unter 06074 4868-0.

### Garantierte Kurstermine

Für Ihre Planungssicherheit bieten wir stets eine große Auswahl garantierter Kurstermine an.

### Ihr Kurs maßgeschneidert

Diesen Kurs können wir für Ihr Projekt exakt an Ihre Anforderungen anpassen.

### Cisco Digital Learning & Cisco U.

Die multimodalen Schulungen der Cisco Digital Learning Library beinhalten referenzengeführte HD-Videos mit hinterlegtem durchsuchbarem Text und Untertiteln, Übungen, Labs und erklärenden Text sowie Grafiken. Das Angebot stellen wir Ihnen über unser Lernportal myExperTeach zur Verfügung. Der Zugriff auf die Kurse steht ab der Freischaltung für einen Zeitraum von sechs Monaten zur Verfügung. Bei Paketen (Cisco U.) beträgt dieser Zeitraum zwölf Monate.

### Cisco Digital Learning & Cisco U. Preise zzgl. MwSt.

6 Monate Freischaltung € 800,-

### Training Preise zzgl. MwSt.

Termin/Kursort	Preis
<b>Termine in Deutschland</b>	<b>4 Tage € 3.195,-</b>
<b>Termine in Österreich</b>	<b>4 Tage € 3.195,-</b>
<b>Termine in der Schweiz</b>	<b>4 Tage € 3.895,-</b>
<b>Online Training</b>	<b>4 Tage € 3.195,-</b>
Kurssprache Deutsch	
08.07.-11.07.24  Online	21.10.-24.10.24  Online
08.07.-11.07.24  Wien	21.10.-24.10.24 Zürich
21.10.-24.10.24  Frankfurt	



# Inhaltsverzeichnis

## SESA – Securing Email with Cisco Email Security Appliance

### Email Security Training

#### 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

#### 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

#### 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

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

#### 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 to Enforce Email Policies

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

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

#### 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

#### 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

#### 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

### 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

#### 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

#### References

Model Specifications for Large Enterprises  
Model Specifications for Midsized Enterprises and Small-to-Midsized Enterprises or Branch Offices  
Cisco Email Security Appliance Model Specifications for Virtual Appliances  
Packages and Licenses

