



Collaboration Security Administrator for the AI Era

The Proofpoint Collaboration Security Administrator certification course builds advanced administrative expertise in utilizing Proofpoint's comprehensive suite, focusing on the day-to-day operations and tasks carried out by those administering Proofpoint platforms. This course dives into many of the Proofpoint products used to safeguard your organization from sophisticated email threats.

Facilitated by our experienced instructors and with practical engaging labs this advanced hands-on course will equip you to administer and manage products like Email Protection, Targeted Attack Protection, Cloud Threat Response, Proofpoint's AI Satori Abuse Mailbox Agent, and Closed-Loop Email Analysis & Response.

Course Syllabus

Proofpoint Products Overview: In this lesson, you will learn how to:

- Identify the different Proofpoint Collaboration Security tools and products
- Understand the fundamental principles governing how each tool functions
- Describe how these tools integrate and interact with one another

Mail Flow: In this lesson, you will learn how to:

- Understand mail routing and how inbound and outbound mail routes are configured
- Explain the purpose of mail relay

COLLABORATION SECURITY ADMINISTRATOR

Format:

Virtual Instructor Led Training (VILT),
Onsite Training At A Customer's
Facilities (OS)

Duration

4
days

Intended Audience:

Messaging,
Administrators, and
Security Analyst

Message Processing: In this lesson, you will learn how to:

- Understand how the Protection Server processes mail and how Proofpoint Dynamic Reputation informs filtering decisions
- Explain SMTP communication and session processing within the Protection Server
- Identify the components of a rule and how Policy Routes, delivery options, and Lists affect message handling
- Describe how policies, rules, and dispositions work together, including disposition precedence and rule firing order
- Configure SMTP Profiles to support specific mail routing needs

Quarantine: In this lesson, you will learn how to:

- Create and delete quarantine folders
- Configure quarantine folder settings
- Search for and release quarantined messages
- Understand quarantine precedence order

Investigation and Logging: In this lesson, you will learn how to:

- Describe the Config Master and agent architecture, and how PPS cluster support message processing and logging
- Use Cloud-Based and On-Prem Smart Search to investigate and troubleshoot mail flow
- Interpret log entry formats and use the Log Viewer to investigate mail flow issues
- Search and filter data within audit logs

Protection Server Monitoring and Reporting: In this lesson, you will learn how to:

- Create alert profiles
- Configure alert rules
- View alerts
- View reports

Encryption: In this lesson, you will learn how to:

- Understand the difference between message-level encryption and TLS
- Identify the connection phases of the TLS handshake
- Enable TLS and enforce TLS to specific domains

User Management and Recipient Verification: In this lesson, you will learn how to:

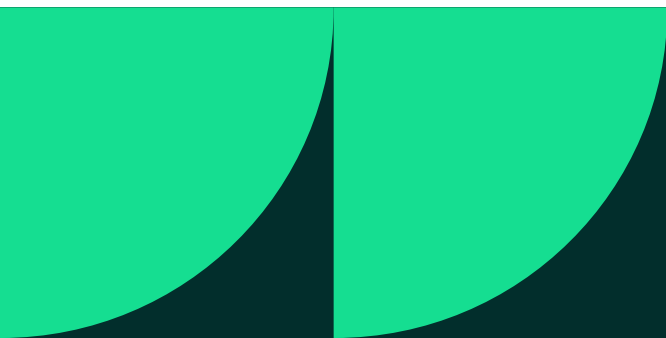
- Understand the PPS User Hierarchy and User Repository, and create Import/Authorization profiles
- Configure Recipient Verification, including Data Connectors, Verification Source Profiles, and Verification Rules
- Add and manage Administrator users across Collaboration Security systems

Email Digests and the End User Web Application: In this lesson, you will learn how to:

- Understand Email Digests and the differences between digest types
- Enable and configure Email Digests
- Enable and configure the Web-based Command Processor and End User Web Application

Email Firewall – More Rules and Functions: In this lesson, you will learn how to:

- Recognize key built-in Email Firewall rules and apply best practices for their use
- Create and manage Dictionaries to mitigate offensive or unwanted content
- Configure Bounce Management to reduce backscatter mail
- Understand and configure SMTP Rate Control and Outbound Throttle settings



Email Authentication: In this lesson, you will learn how to:

- Understand the fundamentals of SPF, DKIM, and DMARC
- Configure SPF, DKIM, and DMARC policies and rules
- Use Smart Search to review email authentication results

Spam Detection: In this lesson, you will learn how to:

- Describe spam scoring, classification, and recommended rule configurations
- Use Threat Protection APIs to manage Safe List and Block List entries
- Identify, report, and troubleshoot false positives and negatives

Virus Protection: In this lesson, you will learn how to:

- Understand the purpose and operation of the Virus Protection Module
- Create Virus Protection Policies
- Create and edit Virus Protection Rules

Email Warning Tags: In this lesson, you will learn how to:

- Understand the purpose of Email Warning Tags
- Understand tag precedence
- Customize Email Warning Tags

Targeted Attack Protection (TAP): In this lesson, you will learn how to:

- Understand the purpose of URL Rewrite and enable and configure it
- Understand the purpose of Message Defense and enable and configure it
- Use TAP Dashboard tools, including URL Decoder, Blocklists, and user privilege management
- Create and use TAP Dashboard API keys to extract data

Threat Response: In this lesson, you will learn how to:

- Differentiate between Cloud (CTR) and On-Prem (TRAP) Threat Response, and review the Messages and Incidents dashboards
- Configure mail servers, Quarantine Modes, and automation workflows in Threat Response
- Understand the CLEAR process and use APIs to manage incidents and messages

Discover the proofpoint platform

<https://www.proofpoint.com/us/cybersecurityacademy>

proofpoint