Enterprise Privacy for the Administrator

Overview

This course covers the Privacy tools that are available as part of the Proofpoint Suite, including modules on Regulatory Compliance, Encryption, and Digital Assets. It also includes topics such as master-agent architecture, installation and deployment, filtering, and rule creation.

Format

Web-based Training (WBT)

Duration

2 hours

Price

Free for Proofpoint customers

Intended Audience

This course is recommended for system administrators, network managers, and information security managers responsible for ongoing management of Proofpoint systems.

Prerequisites

Experience with Enterprise Protection/Privacy and familiarity with the interface is helpful, but not required.

Registration

To access this course, you need a training account. A training account can be requested through CTS by any existing CTS contact at your company (select Other – Training in the Component field), or you can contact your sales representative for help getting a training account set up.

Recommended Follow-up Courses

After successfully completing this course, you may wish to explore the courses below:

- Enterprise Protection for the Administrator
- Enterprise Protection/Privacy Professional Engineer

Course Outline

Welcome and Email

- History of Email
- SMTP Protocol
- Simple SMTP Session

Architecture

- Protection server characteristics
- Server hardware
- Master / Agent Deployment Appliance types
- Physical Appliance Deployment
- Virtual Machine Deployment
- Software Based Deployment
- Alternate Appliance Types

Installation and Deployment

- Setting up a cluster
- Operating system
- Proofpoint specific software
- Third party software
- Building / Re-imaging
- Activating
- Simulation: The Activation Process

Navigation

- Getting started
- How to navigate the management GUI
- Appliance administrators
- Simulation: Creating a new admin account

Filtering

- The Filter
- Order of arrival
- Module precedence order
- Delivery precedence order
- Filter data flow

Rule Creation

- Introduction to rule creation
- Policy routes
- Simulation: Updating an outbound policy route
- Conditions
- Quarantine
- Disposition types
- Create efficient rules
- Custom spam rules
- Simulation: Creating an email firewall rule
- Creating rules
- Tips on creating rules
- Dictionaries

User Repository

- The User Repository
- Introducing users
- Introducing groups
- Assigning attributes for users and groups
- Import/Authentication profiles
- Simulation: Set up an LDAP import profile and test

LDAP

Spam Module

- Spam detection module overview
- Spam module classifiers
- Suspected spam
- Safe/Blocked lists
- Reporting false negatives and positives
- Simulation: Enabling the Audit Quarantine folder

Virus modules

- Multi-layer virus protection
- The zero-hour virus problem
- Simulation: Creating a virus policy that allows a group to send encrypted files

Regulatory Compliance

- Regulatory Compliance Rules
- Creating Dictionaries
- Using Custom Dictionaries
- Smart Identifiers
- Business Partners

Digital Assets

- Documents
- Categories
- Digital Asset Rules
- Incidents and Reports

DKIM, BATV, Web Protection

- Domain Keys Identified Mail
- Using Bounce Address Tag Validation
- BATV Address Format
- ICAP Integration

Encryption

- Proofpoint Encryption
- Authentication
- Key Management
- Message Revocation
- End User Message Revocation
- Proofpoint Encryption Branding
- Allowed Domain List for Secure Reader
- Smart Send

End User Experience

- End user digest
- Enabling and configuring digest messages
- Sample end user digest

- Who receives the digest?
- Simulation: Send a digest to a user
- End user web application
- Self-service in end user web application
- End user authentication
- Authentication sources and options

Reports

- Available reports
- Scheduling and publishing
- Reporting
- Simulation: Publish a report to email automatically