Course Description

# McAfee® Data Loss Prevention Endpoint

**Intel Security Education Services Administration Course Training**

The McAfee® Data Loss Prevention Endpoint Administration course from Intel Education Services provides in-depth training on the tools you need to design, implement, configure, and use McAfee Data Loss Prevention Endpoint to safeguard intellectual property and ensure compliance. The course details how this solution uses McAfee® ePolicy Orchestrator for centralized management. It also explains how to monitor and address day-to-day end-user risky actions such as emailing, web posting, printing, clipboards, screen captures, device control, uploading to the cloud, and more.

## Course Goals

- Plan the deployment.
- Install and configure McAfee Data Loss Prevention Endpoint software on the McAfee ePolicy Orchestrator server.
- Install the McAfee Data Loss Prevention Endpoint client endpoints.
- Use classification, tagging, and protection rules to safeguard sensitive information.
- Locate information with endpoint discovery rules.
- Monitor incidents and events and generate queries and reports.

## Agenda At A Glance

**Day 1**

- Welcome
- Solution Overview
- Planning the Deployment
- McAfee ePO Review
- Preparing the Enterprise Environment
- Installing McAfee DLPe Software
- Permission Sets

## Audience

- This course is intended for system and network administrators, security personnel, auditors, and/or consultants concerned with network and system security.

**Register Now for Training**

intel Security

# Course Description

## Agenda At A Glance Continued

**Day 2**

- Deploying the McAfee DLPe Client Software
- DLP Policy Overview and Client Configuration
- DLP Policy Manager Overview and Initial Configuration
- DLP Privileged Users and End-User Group
- Device Control

**Day 3**

- Content Protection Overview
- Classification and Tagging
- Removable Storage Protection
- Email Protection
- Web Protection
- Printing Protection
- Screen Capture Protection
- Clipboard Protection
- Cloud Protection
- Application File Access Protection McAfee Device Rule Sets and Rules

**Day 4**

- Bring it All Together
- Endpoint Discovery
- Monitoring and Reporting
- Basic Troubleshooting

## Recommended Pre-Work

It is recommended that students have working knowledge of network, system, and security administration is recommended. Prior experience with McAfee ePO is also recommended.

## Course Outline

**Module 1: Welcome**

- Welcome
- About the Course
- Acronyms and Terms in This Course
- Locating Helpful Resources
- Intel Security Expert Center
- Lab Environment

**Module 2: McAfee Data Loss Prevention Endpoint Solution Overview**

- Sources of Data Loss
- Causes of Data Loss
- McAfee Data Loss Prevention (DLP) Portfolio
- Choosing a Data Loss Prevention Solution
- McAfee DLP Endpoint Overview
- New/Enhanced for DLP 9.4X
- How McAfee DLPe Works
  - Classify
  - Track
  - Protect
  - Monitor

**Module 3: Planning a McAfee ePolicy Data Loss Prevention Endpoint Deployment**

- Planning Overview
- Strategy and Goals: Internal Assessment
- Strategy and Goals: Role Assessment
- Strategy and Goals: Technical Assessment
- Strategy and Goals: Risk Assessment
- Strategy and Goals: Privacy Laws
- Classification: Sensitivity
- Classification: Methods
- Classification Scenario: Organizational Level

**McAfee. Part of Intel Security.**
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com

## Course Description

**Module 3: Planning a McAfee ePolicy Data Loss Prevention Endpoint Deployment (Continued)**

- Classification Scenario: Applications
- Classification Scenario: End Users and Clients
- Classification: Find, Apply, and Enforce
- Deployment Planning
- Solution Requirements: ePO Platform
- Solution Requirements: Database
- Solution Requirements: Clients
- Supported Third-party Software
- Pilot Plan
- Post Pilot Validation and Enterprise Rollout
- Other Planning Considerations
- Resource: Deployment Planning Questionnaire
  - ePO Server and Infrastructure Credentials
  - Product-specific Questions
  - Network Requirements
  - McAfee ePO and McAfee Agent
  - Microsoft SQL Server Requirements
  - Client Requirements

**Module 4: Preparing the Enterprise Environment**

- Adding Active Directory Security Groups
- Adding Users to Active Directory Security Groups
- Verifying Active Directory Group Membership
- Preparing Resource Folders
- Configuring Sharing for Resource Folders
- Configuring Permissions for Resource Folders
- Verifying Sharing Settings
- Configuring Custom Permission Entries
- Changing Folder Permissions
- Removing Inheritable Permissions from Parent
- Check Point
- Adding Permission Entries
- Verifying New Permission Entries

**Module 5: McAfee ePolicy Orchestrator Review**

- McAfee ePO Solution Overview
- McAfee ePO Platform Requirements
- Default Ports
- Communications: Tomcat Service
- Logging into the McAfee ePO Web Interface
- Quick Tour of the McAfee ePO Web Interface
- Reporting Options
- Systems Options
- Policy Options
- Software Options
- Automation Options
- User Management Option

**Module 6: Installing McAfee Data Loss Prevention Endpoint Software**

- Obtaining McAfee DLPe Software
- McAfee DLPe Software Overview
- Checking in the McAfee DLPe Package
- Installing the McAfee DLPe Extension
- Installing the McAfee DLPe License
- Verifying the McAfee DLPe Installation

**McAfee. Part of Intel Security.**
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com

## Course Description

**Module 7: Permission Sets**

- Viewing and Editing DLP Server Settings
- Permission Sets Overview
- Adding New DLP Permission Sets
- Default DLP Permissions: Policy Catalog
- Default DLP Permissions: DLP Policy Manager
- Default DLP Permissions: Classifications
- Default DLP Permissions: Definitions
- Default DLP Permissions: Operational Events
- Default DLP Permissions: Case Management
- Help Desk Permissions
- Case Study: DLPe Group Admin
- Case Study: Incident Reviewer
- Case Study: Redaction Reviewer
- Creating Help Desk Permission Sets
- Permissions Exclusive to Administrator
- User Management Review
- Guidelines for Authentication Types
- Creating DLPe Users

**Module 8: Deploying the McAfee Data Loss Prevention Endpoint Clients**

- McAfee DLPe Client Overview
- Deploying Client Software from McAfee ePO Console
- Comparing Client Software Deployment Methods
- Creating Product Deployment Project
- Creating Client Deployment Task
- DLP Endpoint Console

**Module 9: McAfee DLP Policy Overview and Initial Configuration**

- Review:
  - DLP Policies
  - Rules and Rule Sets
  - Definitions
  - Policy Architecture
  - Classification and Tagging
- Policy Overview
- McAfee DLP Client Configuration Policy Operational Modes
  - Device Control and full content protection versus Device Control only
- Data Protection Modules
- Protection Settings: Whitelist
- Content Tracking
- Corporate Connectivity
- Debugging and Logging
- Evidence Copy Service
- Quarantine
- Removable Storage Protection
- Screen Capture Protection
- Web Post Protection
- User Interface Components
- McAfee DLP Policy
- Assigning Active Rule Sets
- Configuring Endpoint Discovery Scan
- Defining Global Settings

**McAfee. Part of Intel Security.**
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com

## Course Description

**Module 10: McAfee DLP Policy Manager Overview**

- McAfee DLP Policy Manager Review
- Rule Sets Tab
- Types of Rules
- Policy Assignment Tab
- Definitions Tab
- Supported Definitions
- Example Data Definitions
- Example Device Control Definition
- Example Definitions: Notification
- Example Definitions: Other
- Example Definitions: Source / Destination
- Other Features

**Module 11: Privileged Users and End-User Group Definitions**

- Overview: Privileged Users, End-User Group Definitions, and Active Directory
- Registering an LDAP Server
- Active Directory Considerations
- Creating Privileged Users
- Example Privileged User
- Defining End-User Group Definitions
- Example End-User Group Definitions
- Multiple User Sessions

**Module 12: Device Control**

- Device Control Overview
- Device Management Overview
- Device Management Overview: Device Classes
- Device Management Overview: Device Definitions
- Device Management Overview: PnP Devices
- Device Management Overview: Removable Storage
- Device Management Overview: Fixed Hard Drive
- Working with Device Classes
- Built-in Device Classes (Read-only)
- Adding New Device Class
- Locating Device GUI
- Working with Device Definitions
- Built-in Device Definitions (Read-only)
- Adding New Device Definition
- Example Conventions: Device Definitions
- Example: File System Definition
- Example: Plug and Play Device Definition
- Example: Removable Storage Device Definition
- Example: Whitelisted Plug and Play Devices
- Overriding Device Class Settings in DLP Policy
- Viewing Incidents

**Module 13: McAfee Device Rule Sets and Rules**

- Device Rule Sets and Rules Overview
- Built-in Device Rule Sets and Rules
- Working with Device Rules
- Device Control Rule Tab
- Adding a Device Rule
- Example Conventions: Device Definitions
- Naming Conventions: Device Rules
- Citrix Device Rule Overview
- Citrix Device Rule Configuration
- Fixed Hard Drive Device Rule Overview
- Fixed Hard Drive Device Rule Configuration
- Plug and Play Device Rule Overview

**McAfee. Part of Intel Security.**
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com

# Course Description

**Module 13: McAfee Device Rule Sets and Rules (Continued)**

- Plug and Play Device Rule Configuration
- Example Removable Storage File Access Device Rule
- Removable Storage File Access Device Rule Configuration
- Removable Storage File Access Device Rule Configuration
- TrueCrypt Device Rule Overview
- TrueCrypt Device Rule Configuration
- Case Studies

**Module 14: Content Protection Overview**

- Data Protection Overview
- Defining a Protection Strategy
- Business Requirements
- Rule Architecture
  - Is Classification Criteria Sufficient?
  - Is Tagging Criteria Needed?
  - What are the Rule Parameters?
  - What is the Desired Result or Outcome?
- Review: Definitions
- Example Conventions
- Data - File Extension Definition
- Notification – Justification Definition
- Notification – User Notification Definition
- Configuring Notification Placeholders
- Application Template Definition
- Email Address Definition
- Local Folder Definition
- Network Address (IP address) Definition
- Network Port Definition
- Network Printer Definition
- Network Share Definition
- Process Name Definition
- URL List Definition
- Window Title Definition
- Bringing it All Together
  - Creating a Protection Rule
  - Naming Conventions: Data Protection Rules

**Module 15: Content Classification and Tagging**

- Classification Review
- Tag Propagation
- Tagging Rules
- More on Tagging
- Creating Classification Criteria
- Example Classifications and Criteria
- Creating Tagging Criteria
- Manual Classification
- Register Documents
- Whitelisted Text

**Module 16: Removable Storage Protection**

- Removable Storage Protection Overview
- Removable Storage Protection Advanced Options
- Protect TrueCrypt Local Disks Mounts
- Portable Devices Handler (Media Transfer Protocol)
- Advanced File Copy Protection
- Deletion Mode
- Removable Storage Protection Use Case
- Example Configuration
- User Notification

**McAfee. Part of Intel Security.**
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com

## Course Description

**Module 17: Email Protection**
- Email Protection Overview
- Client Configuration Guidelines
- Third-party Email Classification
- Use Case
- Example Configuration

**Module 18: Web Protection**
- Web Protection Overview
- Browsers
- Client Configuration Guidelines
- Use Case
- Example Configuration

**Module 19: Printer Protection**
- Printer Protection Overview
- Client Configuration Guidelines
- Use Case
- Example Configuration

**Module 20: Screen Capture Protection**
- Screen Capture Protection Overview
- Applications Protected
- Use Case
- Example Configuration

**Module 21: Clipboard Protection**
- Clipboard Protection Overview
- Use Case
- Example Configuration

**Module 22: Cloud Protection**
- Cloud Protection Overview
- Use Case
- Example Configuration

**Module 23: Application File Access Protection**
- Application File Access Protection Overview
- Use Case
- Example Configuration

**Module 24: Endpoint Discovery**
- Endpoint Discovery Overview
- Running the Discovery Crawler
- Verifying Discovery Settings
- Discovery Rule Sets and Rules
- Demonstration
- Creating a Discovery Rule
- Scheduler Definition
- Creating Scheduler Definition
- Example Scheduler Definition
- Scheduler Definition Fields
- Naming Conventions: Endpoint Discovery Rules
- Setting up a Discovery Scan
- Example Endpoint Scan Configuration
- Quarantined Files or Email Items

**Module 25: Monitoring and Reporting**
- DLP Incident Manager
- DLP Incident Manager: Incident List
- DLP Incident Manager: Incident Tasks
- DLP Incident Manager: Incident History
- DLP Operational Events
- Creating Set Reviewer Rule
- Creating Automatic Mail Notification Rule
- DLP Case Management
- Creating Cases
- Create a Set Reviewer Task
- DLP Server Tasks
- Working with Server Tasks
- Queries Overview
- Data Loss Prevention Queries
- Creating Queries
- Data Loss Prevention Reports

**McAfee. Part of Intel Security.**
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com

**Module 25: Monitoring and Reporting (Continued)**

- Creating Reports
- Working with Reports
- DLP Dashboards
- DLP Dashboards
- Working with Dashboards and Monitors

**Module 26: Basic Troubleshooting**

- Diagnostic Tool Overview
- Generating Client Bypass Key
- Diagnostic Tool Layout and Design
- General Information Tab
- DLPE Modules Tab
- Data Flow Tab
- Tools Tab
- Process List
- Devices Tab
- Active Policy Tab
- Policy Tuning: High CPU Use
- Policy Tuning: Tagging
- Debug Logging



**McAfee. Part of Intel Security.**
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com