COURSE DESCRIPTION

McAfee Network Data Loss Prevention Administration

Education Services administration course

The McAfee® Data Loss Prevention Administration course enables attendees to receive in-depth training on the benefits of the centralized management and deployment of McAfee network data loss prevention products, including McAfee DLP Manager, McAfee DLP Prevent, McAfee DLP Discover, and McAfee DLP Monitor. Enabling administrators to fully understand the capabilities of their security solution not only reduces the risks of misconfiguration, but also ensures that an organization gets the maximum protection from installation and usage. At the end of this course, attendees should understand the capabilities of McAfee Network DLP products and have the ability to install and configure McAfee Network DLP Manager, McAfee DLP Prevent, McAfee DLP Discover, and McAfee DLP Monitor in a production environment. Students will also learn how to customize policy, generate reports and optimize their data loss prevention environment.

Audience

System and network administrators, security personnel, auditors, and/or consultants concerned with network and system security should take this course.

Course Goals

- Installation and administration of McAfee Network Data Loss Prevention appliances
- Case-based policy configuration and deployment
- Incident management and case workflow
- Policy tuning and best practices
- Reporting

Agenda at a Glance

Day 1
- About the Course
- McAfee DLP Overview
- McAfee Network DLP Product Offerings
- McAfee DLP Common Elements
- Case Studies
- McAfee DLP Installation
- McAfee DLP Manager
- McAfee DLP Users and Groups

Day 2
- McAfee DLP Policies
- McAfee DLP Rules
- Rule Content
- Rule Context
- Other McAfee DLP Rule Elements
- Action Rules
- McAfee DLP Monitor
- McAfee DLP Policy

Day 3
- McAfee DLP Discover
- McAfee DLP Discover Policy
- McAfee DLP Email Prevent
- McAfee DLP Email Prevent Policy
- McAfee DLP Web Prevent
- McAfee DLP Web Prevent Policy

Day 4
- Incident Management
- Dashboard and Reporting
- Rule Tuning and Best Practices
- Case Study Review

Course Outline

Module 1: Connected Security and McAfee ePolicy Orchestrator® Overview Security Evolution

- Course Overview
- Facilities
- Introductions
- McAfee Education Services
- McAfee Product Training
- Foundstone® Security Education
- McAfee Technical Support
- McAfee Security Content Release Notes
- Product Enhancement Request
- McAfee Community
- Helpful Links
- Classroom Lab Setup
- Using the Lab Guide

Recommended Pre-Work

It is recommended that students have a working knowledge of Microsoft Windows administration, system administration concepts, a basic understanding of computer security concepts, and a general understanding of viruses and antivirus technologies.

- Resources
- Acronyms and Terms
- McAfee Network DLP Documentation
- Helpful Links to Bookmark

Module 2: McAfee DLP Overview

- The Borderless Business
- Environment
- Data Breaches in the Headlines
- Data Breaches Don't Discriminate
- Data Concerns
- The Costs Involved in Data Loss
- Key McAfee DLP solution requirements
- Data Loss Vectors
- "We All Contribute to It."
- The McAfee Approach
- Data Concerns
- The Costs Involved in Data Loss
- Product Documentation Source

Module 3: McAfee Network DLP Product Offerings

- McAfee DLP Solution Offering
- McAfee DLP Products
- McAfee Network DLP Ports
- Supported Systems
- Compatible McAfee Products
- Supported Repositories
- Supported Browsers
- Supported Languages
- McAfee Network DLP Manager
- McAfee Network DLP Monitor
- Capturing Data
- Mirror Port and Network Tap
- McAfee Network DLP Discover
- McAfee DLP Discover
- McAfee Network DLP Prevent
- McAfee Network DLP Prevent (Email)
- McAfee Network DLP Prevent (Web)
- Deployment Checklist
- Connectivity Requirements and Limitations
- Implementation Process Checklist
- McAfee Change Control

Module 4: McAfee DLP Common Elements

- Policy and Rule Checking
- Policies
- Policy Configuration
- McAfee Network DLP Capture Database
- Case Management
- McAfee Network DLP Case Workflow
- Dashboard and Reporting
- Dashboard
- Search List—Results
- Lab Exercises

Module 5: Case Studies

- Deployment Scenarios
- Main DLP Drivers for Healthcare
- Healthcare Use Case
- Healthcare Information to Protect
- Main DLP Drivers for Manufacturing
- Chemical Manufacturer Case
- Chemical Information to Protect
- Main DLP Drivers for Banking
- Data Breaches—Larger Organizations
- Banking Case
- Banking Information to Protect

Module 6: McAfee DLP Installation

- McAfee DLP Hardware
- McAfee Network DLP Physical Appliances
- McAfee DLP Hardware
- McAfee Network DLP Server Ethernet Ports
- VMware
- McAfee Network DLP Images
- McAfee Network DLP Boot Menu—4400/5500/ Virtual
- Software Install/Upgrade (Utilities for Install)
- Software Install/Upgrade (Utilities for Install)
- Steps to Install McAfee DLP Software
- Switching on the Appliance for the First Time
- McAfee Network DLP Manager Initial Configuration
- McAfee Network DLP Configuration
- Installation Troubleshooting
- Implementation Process Checklist
- McAfee Change Control

Module 7: McAfee DLP Manager

- What is McAfee Network DLP Manager?
- McAfee Network DLP Manager Key Features
- McAfee Network DLP Manager Best Practices
- Firewall Configuration (Port Information)
- Firewall Configuration (Port Information)
- McAfee Network DLP Manager UI—HOME
- McAfee Network DLP Manager UI—INCIDENTS
- McAfee Network DLP Manager UI—CASE
- McAfee Network DLP Manager UI—SEARCH
- McAfee Network DLP Manager UI—POLICIES
- McAfee Network DLP Manager UI—CLASSIFY
- McAfee Network DLP Manager UI—SYSTEM
- McAfee Network DLP Manager UI—Adding a New Device
- McAfee Network DLP Disaster Recovery Features
- Lab Exercises

Module 8: McAfee DLP Users and Groups

- McAfee DLP Users and Groups
- Managing Users and Groups
- Failover Account
- Users
- Adding a New Local User

- Groups
- Groups and Business Units
- McAfee Network DLP Group Properties
- Task Permissions
- Policy Permissions
- McAfee Network DLP LDAP User
- Create a Directory Server
- Adding a LDAP User
- Logging in with LDAP User
- Troubleshooting Directory Server Issues
- Troubleshooting Directory Server Issues
- McAfee Login Collector (MLC)
- Creating McAfee Login Collector
- Lab Exercises

Module 9: McAfee DLP Policies

- McAfee Network DLP Policy
- Policy Configuration
- Policy Definition
- Regional Policy Selection
- Policy Actions
- Activating and Deactivating a Policy
- Creating a Policy—Add Policy Screen
- Creating a Policy—Edit Policy Screen
- Policy Ownership
- Policies and Rules
- Searching
- Policy Advanced Settings
- Lab Exercises

Module 10: McAfee DLP Rules

- Rule Checking
- Rule Definitions
- Rule Tabs
- Adding (Creating) a Rule From a Search
- Rule Creation
- Rule Management
- Define
- Action
- Exceptions
- Restricting Data Matches

Module 11: Rule Content

- Rule Content
- Templates
- Keyword
- Keywords and Stems
- Content Type
- Combining Multiple Definitions
- Using Templates
- Expressions
- Commonly Used Expressions
- In McAfee Network DLP Concepts, What Are \k and \K User For?
- Expression Examples

- Using Expressions
- Concept
- Concepts
- Adding a Concept
- Concept Algorithms
- Managing Concepts
- Duplicating Concepts

Module 12: Rule Context

- Context
- Adding Context to a Concept
- Count
- Percentage Match
- Location
- Proximity—Distance
- Proximity
- Proximity Order
- Concept Example
- Context Examples
- Lab Exercise

Module 13: Other McAfee DLP Rule Elements

- Other Rule Elements
- Source/Destination
- Email Addresses
- IP Address
- URL Match
- GeoIP Location
- File Information
- Document Properties
- Adding a Document Property
- Protocol/Port
- Discover
- Date/Time
- Lab Exercises

Module 14: Action Rules

- Action Rules
- Adding a new Action Rule
- Email Options
- Syslog
- Incident Reviewer
- Incident Status
- Action Rules
- McAfee Network DLP Rule Actions
- Lab Exercises

Module 15: McAfee DLP Monitor

- What is McAfee Network DLP Monitor?
- McAfee Network DLP Monitor
- Using Multiple Monitors
- Monitor Architecture
- Mirror Port/Network TAP
- Capture Filters
- Network and Content Filters
- Network Filter Action Types

- Sample Network Capture Filter
- RFC 1918
- Content Filter Action Types
- Sample Content Capture Filter
- Searching from the GUI
- Search Tasks Permissions
- Basic Search—Example
- Advanced Search—Example
- Search list—Details
- Search list—Results
- Search Tasks
- McAfee Network DLP Appliance Installation
- Quick Start Wizard
- Registering McAfee Network DLP Appliances
- McAfee Network DLP Appliance Registration
- Lab Exercises

Module 16: McAfee DLP Policy

- Data-in-Motion Policy
- Data-in-Motion Action Rules
- Data-in-Motion Policy
- DiM Search Results
- Checking the RFS Disk Space
- Disk Usage
- Troubleshooting—Data Not Being Captured
- Troubleshooting—Check Port Configuration
- Troubleshooting—Network
- Troubleshooting—Check Filters
- Troubleshooting—Summary
- Lab Exercises

Module 17: McAfee DLP Discover

- Scans
- McAfee DLP Discover
- Supported Repositories
- Supported Databases
- McAfee DLP Discover Architecture
- Scan Types
- Four Types
- Concurrent Scan Tasks and Crawl Rate
- Inventory Scans
- Firewall Configuration (Port Information)
- Classification Scans
- Registration Scans
- Data Registration
- About Signatures
- Description of Signature Types
- Discover Scans
- Discover Scan Remediation
- Before Setting Up a Scan
- Adding Discover to McAfee DLP Manager
- Lab Exercises

Module 18: Discover Policy

- McAfee Network DLP Discover Scans
- Schedules
- Credentials
- Export Locations
- SSL-Enabled Database Crawling
- Scan Actions
- Scan States
- Scenario—Creating scanning for PII
- Inventory Scan
- Node Definition
- Checking Credential for a Single IP
- Node Definition Filtering
- Filters
- Advanced Options
- Advanced Options—Rate Control
- Running a Scan
- Scan Results
- Classification Scan
- Data Classification
- Classification Scan—Data Classification
- Predefined View—OLAP Navigator
- McAfee DLP Discover Scan
- McAfee DLP Discover Scan Policies
- McAfee DLP Discover Scan Remediation
- Action Rule Remediation
- Incident Remediation
- Registration Scan
- Lab Exercises

Module 19: McAfee Network DLP Email Prevent

- What is McAfee Network DLP Email Prevent?
- Architecture: McAfee Network DLP Email Prevent
- McAfee Network DLP Email Prevent Redundancy
- Deployment Guidelines—McAfee Network DLP Email Prevent
- Firewall Configuration (Port Information)
- Prevent Network/Content Filters
- Steps to Integrate McAfee Email Gateway with McAfee DLP Prevent
- McAfee Email Gateway Policy—Direct to McAfee Network DLP Email Prevent
- McAfee Email Gateway Policy—Custom Header Dictionary
- McAfee Email Gateway Policy—Post McAfee Network DLP Email Prevent Policy
- McAfee Email Gateway Compliance Rules
- McAfee Network DLP Prevent MTA Access
- Lab Exercises

Module 20: McAfee Network DLP Email Prevent Policy

- McAfee Network DLP Email Prevent
- McAfee Network DLP Email Prevent Actions
- Allowed Actions for McAfee Network DLP Email Prevent

- McAfee Network DLP Email Prevent Policy Flow
- McAfee Network DLP Policy Configuration
- McAfee Network DLP Action by Appliance
- McAfee Network DLP Prevent Policy
- McAfee Network DLP Prevent Troubleshooting
- Tcpdump
- Mailq
- Maillog
- Lab Exercises

Module 21: McAfee Network DLP Web Prevent

- What is McAfee Network DLP Web Prevent?
- Data Flow
- McAfee Network DLP Web Prevent Redundancy
- Deployment Guidelines—McAfee Network DLP Web Prevent
- Firewall Configuration (Port Information)
- Steps to Integrate McAfee Web Gateway with McAfee DLP Prevent
- Add Library Rule
- Rule Set Position
- Data Loss Prevention with ICAP Rules
- ReqMod Setting

Module 22: McAfee Network DLP Web Prevent Policy

- McAfee Network DLP Web Prevent Policy
- McAfee Network DLP Web Prevent Block Page
- McAfee Network DLP Web Prevent Policy
- www.csm-testcenter.org
- McAfee Network DLP Web Prevent Troubleshooting
- Tcpdump
- Lab Exercises

Module 23: Incident Management

- Case Management
- McAfee Network DLP Incident Management
- Supported Incident Types
- Incident Management—Managed Appliances
- Incident Management on the Manager
- Incident Dashboard—Incident Types
- Incident Viewing Formats
- Viewing Incidents in Different
- Formats
- Viewing Incidents in Different Formats
- Incident Actions
- Incident Dashboard Options
- Incident Views and Scheduled Reports
- Policy Permissions for Incidents
- Incident Remediation Workflow
- Case and Incident Management
- Creating a Case
- Creating a Case from Incidents
- Adding Incidents to an Existing Case
- Customize Case Config Option

- Customize Case Config Page
- Case Attachment
- Case Management Permissions
- Case Level Permissions
- Group Task Permissions for Cases
- Case Permissions—Summary
- McAfee Network DLP Case Workflow
- Case Management Best Practices
- Case Management WorkflowExample
- Lab Exercises

Module 24: Dashboard and Reporting

- Dashboard and Reporting
- Predefined Table and Charts
- Risk Analysis Chart
- Customizing Home Page and Charts
- Network Statistics
- Exportable Incidents
- Exportable Cases
- Exportable Searches
- Customizing Export Data
- Lab Exercises

Module 25: Rule Tuning and Best Practices

- False Positives
- Reducing False Positives
- Network Filters
- Content Filters
- Policy—Suppress Incidents
- Rule Modification
- Rule Tuning
- Rule Tuning—Proximity
- Rule Best Practices

Module 26: Case Study Review

- Deployment Scenario Review
- McAfee Medical Services
- Healthcare—Consolidate Files
- Healthcare—Restrict File Transmission
- McAfee Chemical Corporation
- Chemical Company—Notify IP detection
- Chemical Company—Allow PI transmission
- McAfee Federal
- Banking—Rule Sensitivity
- Banking—Incident/Case Management

Learn More

To order, or for further information, please call 1 888 847 8766 or email **SecurityEducation@mcafee.com**.

McAfee™
Together is power.

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

McAfee and the McAfee logo, ePolicy Orchestrator, and Foundstone are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others. Copyright © 2017 McAfee, LLC. 3547_0917
SEPTEMBER 2017