

McAfee Host Intrusion Prevention Administration Course

Education Services administration course

The McAfee® Host Intrusion Prevention Administration course provides attendees with in-depth training on the deployment and management of a host intrusion prevention solution, using McAfee® ePolicy Orchestrator® (McAfee ePO™) software. In addition, attendees will learn how this solution uses a series of device protection, tagging, and reaction rules to safeguard sensitive information and improve overall data security.

Audience

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

Course Goals

- Understand the benefits and capabilities of a McAfee Host Intrusion Prevention solution.
 - Plan and implement the McAfee Host Intrusion Prevention.
 - Use rules, policies, and signatures.
 - Provide zero-day protection for operating system and application vulnerabilities.
 - Reduce the overhead of patch management.
 - Install, configure, and manage the solution, using the McAfee ePO management console.
-

COURSE DESCRIPTION

Agenda at a Glance

Day 1

- Introduction to McAfee Host Intrusion Prevention
- Connected Security and McAfee ePO Overview
- Managing Dashboards and Monitors
- McAfee Agent
- Installing McAfee Host Intrusion Prevention Server
- Windows McAfee Host Intrusion Prevention Client

Day 2

- McAfee Host Intrusion Prevention General Policies
- Intrusion Prevention System (IPS) Policies
- IPS Rules Policies
- Application Protection
- Configuring IPS Exceptions
- Working with IPS Events

Day 3

- Creating IPS Client Rules
- Custom Signatures
- Automatic Responses and Threat
- Notification
- Firewall Policies Overview
- Firewall Rule Policies

Day 4

- Firewall Rule Groups
- McAfee Host Intrusion Prevention Maintenance
- Implementation
- Client Control Utility
- Linux Client
- Solaris Client
- Troubleshooting

Recommended Pre-Work

It is recommended that the students have a working knowledge of Microsoft Windows administration, system administration concepts, a basic understanding of computer security concepts, and a general understanding of Internet services.

Course Outline

Module 1: Introduction to McAfee Host Intrusion Prevention

- Vulnerabilities, Exploits, Buffer Overflows, Attacks, Threats
- Protection Levels
- McAfee Host Intrusion Prevention
- Components and Features
- Supported Operating Systems
- New Features

Module 2: Connected Security and McAfee ePO Overview

- Introducing Connected Security
- Manifestation of Connected Security
- Connected Security Framework
- Integration with Third-Party Products
- Connected Security Solution Platform
- Solution Overview
- New for this Release
- Basic Solution Components

COURSE DESCRIPTION

- Web Interface
- Menu Pages
- Customizing the User Interface
- Architecture and Communication
- User Interface
- Functional Process Logic
- Data Storage

Module 3: Managing Dashboards and Monitors

- Dashboards Overview
- Accessing the Dashboards Page
- Types of Dashboards
- Duplicating and Adding Dashboards
- Assigning Dashboard Permissions
- Dashboard Permissions Guidelines
- Deleting a Dashboard
- Adding Monitors to a Dashboard
- Dashboards Server Settings
- Editing the Automatic Refresh Interval
- Assigning Default Dashboards
- Configuring Dashboard Monitors
- Resizing, Moving, and Removing Monitors
- Concurrent Users (Console Connections)
- Results of Load
- Designing Dashboards
- Changing the Default Session Timeout

Module 4: McAfee Agent

- Agent Components
- Agent-Server Secure Communication Keys
- Communication after Agent Installation
- Typical Agent-to-Server Communication
- McAfee Agent-to-Product Communication
- Forcing Agent Activity from Server
- Wake-Up Calls and Wake-Up Tasks
- Locating Agent Node Using DNS
- Using System Tray Icon
- Forcing McAfee Agent Activity from ClientAgent Files and Directories
- Using Log Files
- Installation Folders

Module 5: McAfee Host Intrusion Prevention Server Planning and Installation

- McAfee Host Intrusion Prevention Installation on the McAfee ePO Server
- Requirements
- Extensions
- Adding Software to the Master Repository
- Software Manager
- Installing McAfee Host Intrusion Prevention Extensions on the McAfee ePO Server
- Checking in the McAfee Host Intrusion Prevention Client Package into the Master Repository
- Upgrading and Migrating Policies

COURSE DESCRIPTION

Module 6: Windows McAfee Host Intrusion Prevention Client

- McAfee Host Intrusion Prevention installation requirements
- Installing the Client Remotely using McAfee ePO and Directly on the Client Computer
- Post-Installation Client Changes
- Registry Implementation
- Client Services and Client-Side Component Relationship
- Downgrading and Removing the Client
- Direct Client-Side Management
- Verifying the Client Is Running
- Allowing the Disable of Features
- Enabling Timed Group
- Unlocking the Windows Client Interface
- Responding to Spoof Detected Alerts
- Managing IPS Protection, Rules, Host Firewall Policy Options, and Blocked Hosts List
- Verifying McAfee Host Intrusion Prevention Events are Triggered Correctly
- Client Logging and Troubleshooting
- Investigating Performance Issues

Module 7: McAfee Host Intrusion Prevention General Policies

- General Policies Overview
- Configuring the Client User Interface Policy
- Configuring Display Options

- Enabling Advanced Functionality and Client Control
- Trusted Networks Policy and Trusted Application
- Creating and Editing Executables
- Working with Multiple Instance Policies
- Marking Applications as Trusted

Module 8: Intrusion Prevention Policies

- Intrusion Prevention Overview
- Benefits of McAfee Host Intrusion Prevention
- IPS Options, Protection, Rules
- Configuring IPS Options
- Using Preconfigured Policies
- Creating and Editing Policies
- Setting Protective Reaction for Signature Severity Levels
- Moving from Basic to Advanced Protection

Module 9: IPS Rules Policies

- Overview of the IPS Rules
- Host Intrusion Prevention Clients
- IPS Protection with IPS Rules Policies
- Host and Network IPS Signature Rules
- Signature and Behavioral Rules
- Signatures and Severity Levels
- Working with IPS Rules Policies and Signatures
- Multiple Instance Policies
- Effective Policy for IPS Signatures
- Multiple Instance Policies and the Effective Policy

COURSE DESCRIPTION

- McAfee VirusScan® Access Protection and IPS Rules

Module 10: IPS Rules Policies—Application Protection

- Application Blocking and Hooking
- Prevent an Executable from Running (Black List)
- Create, Editing, or Viewing Executable Details
- Blocking and Allowing Application Hooking
- Customizing and Managing Rules
- Process Hooking

Module 11: Configuring IPS Exceptions

- Exception Rules
- Configuring IPS Rules Exceptions
- Creating Exceptions for Network IPS Rules
- Applying OS Patches
- Creating Trusted Applications
- Adjusting Signature Severity Levels
- Tuning Methods

Module 12: Working with IPS Events

- Events and Event Logging
- List of the McAfee Host Intrusion Prevention Events Supported by McAfee ePO
- Reacting to Events
- Viewing McAfee Host Intrusion Prevention Events
- Filtering Events
- Creating an Exception Based on a Selected Event
- Analyzing Events

- Viewing Systems on Which Selected Events Occur
- Viewing Common Vulnerabilities and Exposures (CVE) Information
- Creating Event-Based Exceptions
- IPS Signature Events
- General Methodology for Reviewing Updates, Patch Systems, and Applications

Module 13: Creating IPS Client Rules

- IPS Client Rules Overview
- Refining Policies Based on Use
- Learning Mode
- Adaptive Mode
- Placing Clients in Adaptive or Learn Mode
- Adaptive Mode Sequence
- Managing IPS Client Rules
- Create Exceptions Using IPS Client Rules
- Reviewing Detail for IPS Client Rules
- Retaining Existing Client Rules
- Using the Property Translator Server Task

Module 14: Custom Signatures

- Custom Signatures Overview
- Methods for Creating Custom Signatures
- Creating a Custom Signature
- Using the Signature Creation Wizard
- Creating Windows/Unix Files and Directories
- Creating Signatures-Windows Registry

COURSE DESCRIPTION

- Using the Linux or Solaris Option to Create Signatures
- Adding and Editing Sub-Rules
- Viewing General Information about Signature
- Editing the Severity Level, Client Exception Permission, and Log Status of a Signature
- Custom Signatures Components
- File Rule Types and Examples
- Troubleshooting Custom Signatures

Module 15: Automatic Responses and Threat Notification

- Threat Notification and Tracing
- Event Types, Formats, and Lifecycle
- Automatic Response Process
- Creating, Editing, Viewing, and Deleting Automatic Responses for Specific Event Types
- Setting Filters, Aggregating Events, and Configuring Rule Actions
- Creating Issues Executing Scheduled Tasks, and Running External Commands
- Variables Used in Notifications
- Creating and Editing Automatic Responses
- Filtering Events
- Throttling and Aggregation
- Default Automatic Response Rules
- Planning Automatic Responses
- Determining Events Forwarding
- Automatic Responses Permission Set

- Managing Issues
- Creating Contacts

Module 16: Firewall Policies

- McAfee Host Intrusion Prevention Firewall Overview
- Firewall Protocol Support
- Allowing Unsupported Protocols and Bridged Traffic
- Understanding the State Table
- Stateful Filtering and Protocol Tracking
- How Firewall Rules Work
- Firewall DNS Blocking
- Working with Firewall Options Policies
- Startup Protection and Protection Options
- TrustedSource/McAfee Global Threat Intelligence

Module 17: Firewall Rules Policies

- Configuring Firewall Policies
- Firewall Rules Console
- Default Policies
- Typical Corporate Environment Policy
- Firewall Groups
- Creating New Firewall Rule
- Using the Firewall Rule Builder
- Using the McAfee Host Intrusion Prevention Catalog
- Adding Rules from the Catalog
- Creating Firewall Rule Groups
- Adaptive Mode versus Learn Mode
- Managing Firewall Client Rules

COURSE DESCRIPTION

- Refining Policies Based on Use
- Responding to Firewall Alerts
- Stateful Filtering in Adaptive or Learn Mode
- Retaining Existing Client Rules
- Firewall Theory
- Basic Design Philosophies
- Firewall Design Considerations
- Firewall Planning

Module 18: Firewall Rule Groups

- McAfee Host Intrusion Prevention Firewall Groups
- Location-Enabled Firewall Groups
- Connection-Aware Firewall Groups
- Matching for Location-Aware Groups
- Timed Groups in Firewall Policy

Module 19: McAfee Host Intrusion Prevention Maintenance

- Server Tasks in McAfee ePO
- Clearing Events
- Generating McAfee Host Intrusion Prevention Reports/Queries
- Reports
- Dashboards and Queries
- Running Predefined McAfee Host Intrusion Prevention Queries
- Creating Custom McAfee Host Intrusion Prevention Queries

- Client-Side Policy Reporting
- Default Dashboards
- Vulnerability Shielding Updates
- McAfee Agent Update Task
- Manual Content Updating
- McAfee Internet Sites
- Creating an McAfee ePO Server Pull Task
- Testing McAfee Host Intrusion Prevention Client
- Adaptive Mode versus Learn Mode
- Managing Firewall Client Rules
- Refining Policies Based on Use
- Responding to Firewall Alerts
- Stateful Filtering in Adaptive or Learn Mode
- Retaining Existing Client Rules
- Firewall Theory
- Basic Design Philosophies
- Firewall Design Considerations
- Firewall Planning

Module 20: McAfee Host Intrusion Prevention Implementation and Best Practices

- Pre-Installation Considerations and Deployment Planning
- Best Practices
- Step 1: Strategy and Planning
- Lab or Real World?
- Confirm Your Rollout Strategy

COURSE DESCRIPTION

- Timing and Expectations
- Preparing the Environment
- Step 2: Prepare the Pilot Environment
- Using McAfee ePO
- Step 3: Installation and Initial Configuration
- Managing Protection
- “Out-of-the-Box” Protection
- Multiple Policy Instances
- Notify End Users and Plan Escape Hatches
- Enlist the Help Desk Team
- Install McAfee Host Intrusion Prevention to Pilot Hosts
- Check Pilot Systems for Proper Operation
- Step 4: Initial Tuning
- McAfee Host Intrusion Prevention Configuration and Initial Tuning
- Tuning Methods
- Fine-Tuning Policies
- Security Tightening
- Follow these Processes
- More Tuning
- Create Exceptions
- Create Trusted Applications
- Run Queries
- Step 5: Optional Adaptive Mode
- Adaptive Mode: Refine Policies Based on Use
- Understanding Adaptive Mode

- Adaptive Mode Limitations
- Best Practices with Adaptive Mode
- Potential Pitfalls in IPS Deployments
- Step 6: Enhanced Protection and Advanced Tuning
- Heightened Protection and Advanced Tuning
- Step 7: Maintenance and Expansion Beyond IPS
- Server Maintenance
- Domain Controllers and McAfee Host Intrusion Prevention

Module 21: ClientControl Utility

- Deploying McAfee Host Intrusion Prevention with Third-Party Product
- ClientControl Logging
- Command Line Syntax
- Major Arguments
- Argument - /help
- Argument - /start and /stop
- Stopping McAfee Host Intrusion Prevention Services
- Argument - /log
- Argument - /engine
- Argument - /export
- Argument - /readNaiLic
- Argument - /exportConfig
- Argument - /defConfig
- Argument - /startupIPSProtection
- Argument - /execInfo

COURSE DESCRIPTION

- Argument - /fwPassthru
- fwinfo Utility

Module 22: Linux Client

- Linux Client Installation Requirements
- Policy Enforcement with the Linux Client
- Notes about the Linux Client
- Removing the Linux Client
- Troubleshooting the Linux Client
- hipts—Troubleshooting Tool
- Verifying Linux Installation Files
- Stopping and Restarting the Linux Client

Module 23: Solaris Client

- Solaris Client Installation Requirements
- Policy Enforcement with the Solaris Client
- Solaris Zone Support
- Installing the Solaris Client
- Removing the Solaris Client
- Troubleshooting the Solaris Client
- hipts—Troubleshooting Tool
- Verifying Solaris Installation Files
- Stopping and Restarting the Solaris Client

Module 24: Troubleshooting McAfee Host Intrusion Prevention Forums and Security Advisories

- Knowledge Base Articles for McAfee Host Intrusion Prevention
- MERTool
- Client Issues
- Identify the Versions
- McAfee Host Intrusion Prevention Engines
- Installation Issues
- McAfee Agent Logs
- Policy, Event, and Client Rule Issues
- Policy Update Issues
- Verifying Policies—Static Configuration
- Verifying Policies—Dynamic Policy
- fwinfo.exe
- Verifying Policies—FireCore Policy
- Troubleshooting McAfee Host Intrusion Prevention
- Troubleshooting the McAfee Host Intrusion Prevention Firewall
- Troubleshooting Firewall Issues
- Activity Log
- Applying Service Packs
- Escalation Process

Learn More

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



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

McAfee and the McAfee logo, ePolicy Orchestrator, McAfee ePO, and VirusScan 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. 3546_0917
SEPTEMBER 2017