

McAfee Application Control and McAfee Change Control Administration

McAfee® Education Services Instructor-led Training

The McAfee® Application Control and McAfee® Change Control Administration course from McAfee Education Services provides in-depth training on the tools you need to efficiently install, configure, operate, and troubleshoot issues relating to McAfee Application Control and McAfee Change Control to safeguard intellectual property and ensure compliance. The course details how this solution uses McAfee® ePolicy Orchestrator® (McAfee® ePO™) software for centralized management. It also explains how to use McAfee Application Control for dynamic allow listing to ensure that only trusted applications run on devices servers, and desktops and how to use McAfee Change Control to monitor and prevent changes to the file system, registry, and user accounts.

Earn up to 32 CPEs after completing this course.*

* Student must self-report for CPE credits. We cannot guarantee any specific quantity, as it is up to the program or certification group to determine what they will or will not accept.

Audience

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

Connect With Us



COURSE DESCRIPTION

Course Goals

- Describe the McAfee Application Control and McAfee Change Control solution.
 - Plan McAfee Application Control and McAfee Change Control deployment.
 - Install and configure McAfee Application Control and McAfee Change Control.
 - Deploy and configure the Solidcore client.
 - Configure server tasks and permission sets.
 - Create and manage policies and rules.
 - Design the McAfee Application Control trust model.
 - Manage the software inventory.
 - Enable and configure McAfee Change Control.
 - Configure Integrity Monitoring policies.
 - Gather and analyze events and alerts.
 - Create and interpret reports.
 - Perform basic troubleshooting.
 - Use the Solidcore command line interface to perform endpoint administration.
 - Identify best practices.
 - Describes Inventory mode.
 - Describes Common Platform Enumeration (CPE).
 - Describes trusted local group.
 - Describes enhancements in 8.3.2 release.
-

Agenda at a Glance

Day 1

- Welcome
- McAfee ePolicy Orchestrator Software Overview
- McAfee Application Control and McAfee Change Control Overview
- Deployment and Extension Install
- Permission Sets
- Solidcore Client

Day 3

- McAfee Application Control Inventory
- McAfee Change Control
- Integrity Monitoring
- Events and Alerts
- Dashboards and Reporting

Day 2

- Application Control Rule Groups and Rules
- Change Control Rule Groups and Rules
- Application Control Policies
- McAfee Application Control Trust Model
- Modify Protected Files

Day 4

- Troubleshooting
 - Administration Using the Command Line Interface
 - Recommended Practices
 - Case Studies
-

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 internet services.

COURSE DESCRIPTION

Learning Objectives

Welcome

This first module provides an overview of course design, logistics, and helpful resources, as well as the opportunity for the instructor to learn about you and your training expectations.

McAfee ePolicy Orchestrator Software Overview

Describes McAfee ePO software basics, how it fits into the connected security model, solution components and features, enhancements, and changes for this software release and architecture.

McAfee Application Control and Change Control Overview

Describe McAfee Application Control and McAfee Change Control components, features, and functionality.

Planning a Managed Deployment and Install MACC Extension

Describe the prerequisites and key parts of a deployment plan, and identify solution considerations and pilot plan phases. Learn how to add the McAfee Application Control and McAfee Change Control extension to the McAfee ePO server and verify installation.

McAfee Application Control and McAfee Change Control Server Tasks and Permission Sets

Identify default permissions sets included with McAfee ePO software, McAfee Application Control, and McAfee Change Control, and understand the product-specific server tasks created after deployment.

Solidcore Client

Describe how to enable and disable Solidcore Client tasks, describe user notifications, events, and approvals, and customize user notifications.

Rule Groups and Rules

Explain rule groups, rule group ownership, and rule groups permissions, configure and manage rule groups, and describe McAfee Application Control, McAfee Change Control, and the Integrity Monitoring rule group tabs.

Application Control Policies

Describe McAfee Application Control policies and their relationship to rule groups, define the role of the policy, and configure policies.

McAfee Application Control Trust Model

Understand the basics of allow listing and design the McAfee Application Control trust model.

Modify Protected Files

Understand how to use Update mode and Observe mode, and describe how to make rule modifications.

McAfee Application Control Inventory

Navigate the Inventory menus, describe how to fetch and manage an Inventory, and explain how to compare an Inventory.

McAfee Change Control

Discuss how to use write protection and read protection in policies, define updaters and authorized users, and configure McAfee Change Control.

COURSE DESCRIPTION

Integrity Monitoring

Configure Integrity Monitoring policies, reduce “noise” using and Advanced Exclusion Filter, and understand how to use content change tracking.

Events and Alerts

Describe how Solidcore events are handled in McAfee ePO software, understand when to use one-click exclusion, and configure Solidcore alerts in McAfee ePO software.

Dashboards and Reporting

View and use Solidcore dashboards and queries, and view Solidcore reports.

Troubleshooting

Identify Client versus McAfee ePO software handling, locate log file and key resources, use troubleshooting tools, and troubleshoot feature implementation issues.

Administration Using the Command Line Interface

Use the command line interface to administer systems not connected to McAfee ePO software.

Recommended Practices

Identify best practices for initial setup, testing, policy creation and tuning, and maintenance.

Case Studies

Create your own McAfee Application Control and McAfee Change Control policies without guidance, and create a notification for violations of these policies.

Learn More

To order, or for further information, please email SecurityEducation@mcafee.com.



6220 America Center Drive
San Jose, CA 95002
888 847 8766
www.mcafee.com

McAfee and the McAfee logo, ePolicy Orchestrator, and McAfee ePO 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 © 2021 McAfee, LLC. 4698_0121 JANUARY 2021