McAfee Application Control/ McAfee Change Control Administration

Education Services Administration Course

The McAfee® University McAfee Application Application Control/McAfee Change Control Administration course enables attendees to receive in-depth training on the full benefits and deployment of McAfee Application Control/McAfee Change Control products. Enabling administrators to fully understand the capabilities of their security solution not only reduces the risks of misconfiguration but also ensures an organization gets the maximum protection from their installation.

Course Goals

- Understand the capabilities of McAfee Application Control/ McAfee Change Control solution
- Install and administer ACCC
- Manage Remote Clients
- Protect end points

Audience

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

Agenda at a Glance

Day 1
- Connected Security and McAfee® ePolicy Orchestrator® (McAfee ePO™) Overview
- Introduction to the McAfee Application Control/McAfee Change Control
- Planning a McAfee AC/CC-McAfee ePO Deployment
- McAfee Agent
- McAfee Application Control/McAfee Change Control Extension Installation
- MACCC McAfee Application Control/McAfee Change Control Server Tasks and Permissions
- Solidcore Clients

Day 2
- Introduction to McAfee Application Control Policies
- Policy Modifications
- Inventory

Day 3
- Events and Alerts
- Introduction to McAfee Change Control and Integrity Monitoring
- Change Control Configuration
- Dashboards and Reporting

Day 4
- Troubleshooting
- Case Studies
- CLI Administration
- Best Practices

Course Outline

Module 1: Introduction to the McAfee Application Control/McAfee Change Control

- What is MACCC?
- Supported Operating Systems
- Solidcore Architecture
- Multilayered Security Solution
- Whitelisting
- Trust Model
- Image Deviation
- Differentiators
- Visibility and Enforcement for End- to-End Compliance
- File Integrity Monitoring
- Change Prevention
- Install Workflow
- Navigation to Solidcore Components
- Solidcore Configuration
- Updaters or Publishers
- Solidcore Configuration
- Installers

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 viruses and antivirus technologies.

- Solidcore Policies
- Windows Path Definitions
- Solidcore Server Tasks
- Solidcore: Purge Task
- Migration Server Task
- Calculate Predominant Observations (Deprecated)
- Content Change Tracking Report Generation
- Solidcore: Run Image Deviation
- Image Deviation (McAfee Application Control)
- Specifying a Golden Image
- Solidcore: Scan a Software Repository

Module 2: Planning a McAfee ePolicy Orchestrator Deployment

- Platform Requirements
- McAfee ePO Server Hardware Requirements
- McAfee ePO Server Operating Systems
- McAfee ePO Server Prerequisite Software
- Supported Web Browsers
- Supported SQL Server Releases
- Default Communication Ports
- Default Ports
- Determining Ports in Use
- Virtual Infrastructure Requirements
- Deployment Guidelines
- Deployment Scenario: Basic Plan
- Solution A: One McAfee ePO Server
- Solution B: Two McAfee ePO Servers
- Solution C: McAfee ePO server with Agent Handlers
- Deployment Scenario: Disk Configuration
- Solution: Less than 5,000 Nodes
- Solution: 5,000 to 25,000 Nodes
- Deployment Scenario: Disk Configuration
- Solution: 25,000 to 75,000 Nodes
- Solution: More than 75,000 Nodes
- Database Sizing
- How Products and Events Affect Calculations
- Example: Calculating Averages
- Calculating Your Environment
- Managing Scalability
- Environmental Factors

Module 3: Security Connected and McAfee ePolicy Orchestrator Overview

- Security Evolution
- Security Connected
- Breadth and Depth for Security
- McAfee ePO Solution Overview
- New for this Release
- Basic Solution Components
- How McAfee ePO Works
- Essential Features
- Integration with Third-Party Products
- McAfee ePO Web Interface

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

Module 4: McAfee Agent

- McAfee Agent Overview
- New for This Release
- Agent Components
- Agent-Server Secure Communication Keys
- Communication after Agent Installation
- Typical Agent-to-Server Communication
- Agent-to-Product Communication
- Forcing Agent Activity from Server
- Wake-Up Calls and Wake-Up Tasks
- Configuring Agent Wake-up
- Locating Agent Node Using DNS
- Using System Tray Icon
- Forcing Agent Activity from Client
- Viewing Agent Log
- McAfee ePO 4.x/Agent 4.x Feature Dependencies
- Agent Files and Directories
- Sitelist.xml
- Agent Log Files
- Using Log Files
- Installation Folders

Module 5: McAfee Application Control/McAfee Change Control Extension Installation

- Extensions in McAfee ePO
- Extensions Menu
- Integration of AC/CC Extension
- Installation Requirements
- System Requirements
- McAfee ePO Database Sizing
- Installation of Extension
- Solidcore Licensing
- What is Solidcore?
- Install Workflow Review
- Installing Licenses
- Solidcore Database Tables

Module 6: Solidcore Client

- Solidcore Architecture
- The Agent Plug-in and How It Works
- Types of Platforms Protected
- Supported Systems
- Check in Agent Plug-In Package into McAfee ePO
- Deploying the Solidcore Agent Plug-In
- Verifying Installation from the Endpoint
- Solidcore Client Tasks
- Enable Solidcore Agent Task
- Disable Solidcore Agent Task
- Initial Scan to Create Whitelist

- Pull Inventory
- Begin Update Mode
- End Update Mode
- Change Local CLI Access
- Collect Debug Info
- Run Commands
- Get Diagnostics for Programs
- Features for the Client
- Client Notifications and Events
- Client Events and Approvals
- Customizing Client Notifications

Module 7: McAfee Application Control Initial Configuration

- What are Observations?
- Observe Mode
- Manage Requests
- Review Requests
- Process Requests
- Allow by Checksum on All Endpoints
- Allow by publisher on All Endpoints
- Ban by Checksum on All Endpoints
- Define Custom Rules for Specific Endpoints
- Allow by Adding to Whitelist for Specific Endpoints
- Define Bypass Rules for All Endpoints
- Delete Requests
- Review Created Rules
- Throttle Observations
- Define the Threshold Value
- Review Filter Rules
- Manage Accumulated Requests
- Exit Observe Mode
- Inventory Introduction
- Fetch Inventory
- GTI Integration
- Trust Level and Score
- Cloud Trust Score
- Inventory Without Access to McAfee GTII
- Fetch McAfee GTI Ratings for Isolated Networks
- Export SHA1s of All Binaries
- Run the Offline McAfee GTI Tool
- Fetch Inventory—Bad File Found Event
- Manage the Inventory
- Manage Binaries
- McAfee Application Control Policies
- Role of the Policy
- McAfee Application Control Configuration
- Managing Rule Groups
- Creating a McAfee Application Control Rule Group
- Updater Tab
- Trusted Users
- Exceptions
- Using a Rule Group to Block an Application

Module 8: Application Control Feature Administration

- What is Update Mode?
- How to Update a Solidified System
- Auto-updaters
- Authorized Updaters
- Determining Updaters
- Understanding Publishers
- Understanding Installers
- Scan a Software Repository
- Revisit—Solidcore Permission Sets
- Reboot Free Activation
- Inventory Management Enhancements
- Inventory Management—Pull Inventory
- Inventory by Application
- Inventory by Systems
- Inventory Application Drill-Down
- Inventory Binary Drill-Down
- Search Filters
- Modifying Enterprise Trust Level

Module 9: Event and Alerts

- Understanding Events
- What Creates an Event
- When Are Events Sent Back?
- Viewing Events
- Advanced Filters
- Selecting Columns to Display
- Viewing the Details of an Event
- Solidcore Events
- Example of Solidcore Events
- McAfee Application Control Events
- Planning Automatic Responses
- Throttling, Aggregation, and Grouping
- Alerts
- Understanding Alerts
- Scenarios
- Configuring a Solidcore Alert
- Viewing an Alert
- Support of SNMP Alerts
- Customizing End-User Notifications
- Syslog Enhancements

Module 10: McAfee Change Control Initial Configuration

- McAfee Application Control and McAfee Change Control
- McAfee Change Control and Integrity Monitoring
- Scenario
- File Integrity Monitoring
- Workflow
- Disable Solidcore
- Enable Solidcore on the Endpoint
- Verifying Client Task Completion

- Integrity Monitoring Policies
- Using Integrity Monitor
- Creating an Integrity Monitor Policy
- Integrity Monitoring Policies
- Testing your Monitoring
- Reducing "Noise"
- Example of Reducing "Noise"

Module 11: Using the Policy Catalog and Managing Policies

- McAfee Change Control Policies
- Role of the Policy
- Variables for Use in Policies
- Example of Variables in a Rule Group
- Scenario
- Write Protect a File, Trusted Program Can Alter
- Write Protect a Registry Key, Program can Alter
- Write Protect a File, Trusted User Can Alter
- Verifying only Trusted User Can Alter
- Read Protection Must Be Enabled
- Read Protect a File, Trusted Program can Access
- Emergency Changes
- Content Change Tracking
- One-Click Exclusion (Advanced Exclusion Filtering)
- One-Click Exclusion Configuration
- Troubleshooting

Module 12: Dashboards and Reporting

- The Dashboard
- McAfee ePO Dashboards
- Queries as Dashboard Monitors
- Dashboard Access
- Dashboard Configuration
- Solidcore Dashboards
- McAfee Application Control Dashboard
- McAfee Change Control Dashboard
- Integrity Monitor Dashboard
- Inventory Dashboard
- Solidcore Queries
- Reporting > Solidcore
- McAfee Application Control > Inventory
- McAfee Application Control > Image Deviation
- Automation > Solidcore Client Task Log
- Scenario
- Creating a Customized Dashboard
- Making a Dashboard Public
- Set the Default Dashboard

Module 13: Troubleshooting

- Solidcore Architecture and Components
- Solidcore 6.1.3 Architecture
- Troubleshooting References
- Location of Solidcore Files on Endpoint

- McAfee ePolicy Orchestrator Application Server Service Logs
- Solidcore Registry Keys on Endpoint
- Solidcore Services
- Troubleshooting Best Practice
- Escalation Best Practices
- Troubleshooting McAfee GTI Cloud Issues Best Practice
- Top Issues—Task Failure
- Top Issues—Denied Execution Issues
- Top Issues—Denied Execution of a Network Share
- Top Issues—Network Share
- Top Issues—KB
- Useful Tools
- Solidcore Event Logs
- Solidcore User Notifications
- Solidcore Troubleshooting Tools
- Escalation Tools
- Solidcore Database Tables
- Minimum Escalation Requirements (MER)
- Running MER Tool on Client
- Dump Tools

Module 14: Case Studies

- A Case from History
- Unpatched, Known Vulnerabilities in the Client
- Browser-Based Exploits
- The Remedy
- Application Whitelisting
- Increasing Compliance Requirements
- Remedy
- File Monitoring
- Complete the Task

Module 15: CLI Administration

- Solidcore CLI
- Location of Solidcore Files on Endpoint
- Viewing the CLI Access
- Enabling the CLI
- Unlocking the CLI Locally
- Securing the CLI
- Using the CLI
- SADMIN Commands
- Solidifying from the CLI
- Unsolidifying
- What is Solidcore's Status?
- Beginning the Update Status
- Ending the Update Status
- Enabling and Disabling Solidifier
- SADMIN Commands
- Advanced SADMIN Commands
- Solidcore Commands
- New CLI Commands
- McAfee Application Control Rules and Helpful Commands

- Read/Write Protect Files
- Change Control Commands—Write Protection
- How to Write Protect a File
- Modifying a Read/Write Protected Files
- Change Control Features—Write Protection
- Application Control
- Authorize Command Arguments
- Discovering and Adding Updaters
- SADMIN Diag Notations
- Discovering and Adding Updaters
- Using Attributes to Control File Execution
- Attributes
- Using Attributes to Control File Execution
- Viewing Solidcore Events
- Event Sinks
- Logging Events
- Event Names and Log Entries
- Product Tools

Module 16: Best Practices

- Review of Initial Setup Tasks
- Systems Tree Infrastructure
- Communication between McAfee ePO and Agent
- Activation Options: McAfee Application Control Only
- Inventory Collection Scan
- Protection State Selection
- Protection State Delivery
- Testing Protection Mechanisms
- Policies and Rule Groups
- Policy Tuning
- Bypass Rules and Exclusions
- Inventory and Whitelist
- Updaters
- McAfee Application Control Memory Protection
- Maintenance
- Basic Troubleshooting and FAQs
- Solving Memory Discrepancies
- Helpful Resources

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