

McAfee Application Control / Change Control Administration

Intel Security Education Services Administration Course



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

Course Goals

- Understand the capabilities of McAfee's Application Control / Change Control solution
- install and administer ACCC.
- Manage remote clients.
- Protect end points.

Agenda At A Glance

Day 1

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

Audience

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



[Register Now for Training](#)

Course Description

Agenda At A Glance Continued

Day 2

- Introduction to Application Control Policies
- Policy Modifications
- Inventory

Day 3

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

Day 4

- Troubleshooting
- Case Studies
- CLI Administration
- Best Practices

- File Integrity Monitoring
- Change Prevention
- Install Workflow
- Navigation to Solidcore Components
- Solidcore Configuration
- Updaters or Publishers
- Solidcore Configuration
- Installers
- 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 (Application Control)
- Specifying a Golden Image
- Solidcore: Scan a Software Repository

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 anti-virus technologies.

Course Outline

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

- What is MACCC?
- Supported Operating Systems
- Solidcore Architecture
- Multi-layered Security Solution
- Whitelisting
- Trust Model
- Image Deviation
- Differentiators
- Visibility and Enforcement for End-to-end Compliance

Module 2: Planning a McAfee® ePolicy Orchestrator™ Deployment

- Platform Requirements
- ePO Server Hardware Requirements
- ePO Server Operating Systems
- 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

Course Description

Deployment Scenario: Basic Plan

Solution A: One ePO Server

Solution B: Two ePO Servers

Solution C: 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

ePO Solution Overview

New for this Release

Basic Solution Components

How ePO Works

Essential Features

Integration with Third-Party
Products

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

McAfee 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 McAfee Agent Activity from
Client

Viewing McAfee Agent Log

ePO 4.x/McAfee Agent 4.x Feature
Dependencies

Agent Files and Directories

Sitelist.xml

McAfee Agent Log Files

Using Log Files

Installation Folders

Module 5: Application Control/Change Control Extension Installation

Extensions in ePO

Extensions Menu

Integration of AC/CC Extension

Installation Requirements

System Requirements

ePO Database Sizing

Installation of Extension

Solidcore Licensing

Course Description

What is Solidcore?	Allow by checksum on all endpoints
Install Workflow Review	Allow by publisher on all endpoints
Installing Licenses	Ban by checksum on all endpoints
Solidcore Database Tables	Define custom rules for specific endpoints
Module 6: Solidcore Client	
Solidcore Architecture	Allow by adding to whitelist for specific endpoints
The agent plug-in and how it works	Define bypass rules for all endpoints
Types of Platforms Protected	Delete requests
Supported Systems	Review created rules
Check in Agent Plug-in Package into ePO	Throttle observations
Deploying the Solidcore Agent Plug-in	Define the threshold value
Verifying Installation from the Endpoint	Review filter rules
Solidcore Client Tasks	Manage accumulated requests
Enable Solidcore Agent Task	Exit Observe mode
Disable Solidcore Agent Task	Inventory Introduction
Initial Scan to Create Whitelist	Fetch Inventory
Pull Inventory	GTI Integration
Begin Update Mode	Trust level and score
End Update Mode	Cloud Trust Score
Change Local CLI Access	Inventory Without Access to GTI
Collect Debug Info	Fetch McAfee GTI ratings for isolated networks
Run Commands	Export SHA1s of all binaries
Get Diagnostics for Programs	Run the Offline GTI tool
Features for the Client	Fetch Inventory – Bad File Found Event
Client Notifications and Events	Manage the inventory
Client Events and Approvals	Manage Binaries
Customizing Client Notifications	Application Control Policies
Module 7: Application Control Initial Configuration	Role of the Policy
What are Observations?	Application Control Configuration
Observe Mode	Managing Rule Groups
Manage requests	Creating an Application Control Rule Group
Review requests	Updater Tab
Process requests	Trusted Users

Course Description

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-Updateers

Authorized Updateers

Determining Updateers

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

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: Change Control Initial Configuration

Application Control & Change Control

Change Control & 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

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

Course Description

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

ePO Dashboards

Queries As Dashboard Monitors

Dashboard Access

Dashboard Configuration

Solidcore Dashboards

Application Control Dashboard

Change Control Dashboard

Integrity Monitor Dashboard

Inventory Dashboard

Solidcore Queries

Reporting > Solidcore

Application Control > Inventory

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

ePolicy Orchestrator Application
Server Service Logs

Solidcore Registry Keys on Endpoint

Solidcore Services

Troubleshooting Best Practice

Escalation Best Practices

Troubleshooting 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

Course Description

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
Application Control Rules & 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 ePO and Agent
Activation Options: 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
Application Control Memory Protection
Maintenance
Basic Troubleshooting and FAQs
Solving Memory Discrepancies
Helpful Resources



To order, or for further information,
please contact McAfee Education
at:
1-866-210-2715.

NA, LTAM, and APAC:
education@mcafee.com

EMEA:
proserv@mcafee.com