McAfee® Drive Encryption Administration Course

The McAfee Drive Encryption Administration course from McAfee Education Services provides attendees with hands-on training on the design, setup, configuration, and management of this application. In addition, students will understand how to effectively implement the software in a complex enterprise.

**Course Goals**
- Install Drive Encryption.
- Synchronize with Active Directory.
- Protect endpoints.

**Agenda At A Glance**

**Day 1**
- Security Connected
- Managing Dashboards and Monitors
- Using the Policy Catalog and Managing Policies
- McAfee Agent
- Overview of Encryption Technologies and Computer Boot Concepts

**Audience**
- System and network administrators, security personnel, auditors, and/or consultants concerned with network and system security should take this course.
Course Description

Agenda At A Glance Continued

Day 2
- Introduction to McAfee Drive Encryption
- ePO Installation of DE
- Active Directory Configuration
- Drive Encryption Users
- Installing DE onto Clients

Day 3
- Offline Activation
- Drive Encryption Policies
- DE Dashboards and Reports
- DE Administrative Users

Day 4
- Troubleshooting DE
- Recovery Configuration
- Disaster Recovery with DETech
- DE Scripting
- Uninstall

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 Outline
About the Course
- Course Overview Intro
- Topics Intro
- Resources Intro
- Acronyms and Terms Intro
- McAfee Education Services Intro
- McAfee Technical Support Intro
- McAfee Security Content Release Notes Intro
- Product Enhancement Request Intro
- McAfee Community Intro
- Helpful Links Intro
- Classroom Lab Topology Intro
- IP Addresses and Credentials Intro
- Using VMware Workstation Intro
- Using the Lab Guide Intro

Module 1: McAfee Security Connected and ePolicy Orchestrator Overview Security Evolution
- The ‘Computer’ Timeline
- McAfee Security Connected
- Breadth and Depth for Security
- ePO Solution Overview
- ePO Basic Solution Components
- Basic Solution Components
- How ePO Works
- Essential Features
- ePO Web Interface
- Interface: Menu Page
- Menu Page Reporting
- Menu Page Systems
- Menu Page Policy
- Menu Page Software
- Menu Page Automation
- Menu Page User Management
- Customizing the User Interface
- Architecture and Communication
- User Interface
- Functional Process Logic
- Data Storage
- Check Your Understanding

Module 2: Managing Dashboards and Monitors
- Dashboards Overview
- Accessing the Dashboards Page
- McAfee Default Dashboards (Read-only)
- Other McAfee Dashboard Options
- Using Dashboards
- Duplicating a Dashboard
- Adding a Dashboard
Module 3: Using the Policy Catalog and Managing Policies
- What is a Policy?
- Policy Catalog Page
- Creating a New Policy
- Editing a Policy
- Duplicating a Policy
- Renaming or Deleting a Policy
- Policy Assignment and Inheritance
- Viewing Policy Assignments
- Locking Assignment and Enforcement
- Assigning Policy to Group System Tree
- Assigning Policy to Single System
- Assigning Policy to Multiple Managed Systems
- Viewing and Resetting Broken Inheritance
- Resetting Broken Inheritance
- Copying and Pasting Assignments
- When Policies are Enforced
- Permission Set for Policies
- Check Your Understanding

Module 4: McAfee Agent
- New for McAfee Agent 4.8
- McAfee Agent
- Agent ComponentsAgent
- Agent ComponentsScheduler
- Agent ComponentsUpdater
- How ePO Server Uses Agent GUID
- Agent-to-Server Communication Interval
- ASCI Communication Interruption Handling
- Agent-to-Server Communication
- Agent-Server Secure Communication Keys
- Communication after Agent Installation
- Typical Agent-to-Server Communication
- McAfee Agent-to-Product Communications
- Forcing Agent Activity from Server
- Wake-up Calls and Wake-up Tasks
- Configuring Agent Wake-up
- Using System Tray Icon
- Forcing McAfee Agent Activity from Client
- Viewing McAfee Agent Log
- Sorting McAfee Agent Log
- Reviewing Agent Log Information
- SuperAgents
Course Description

- SuperAgent Communication
- Agent Files and Directories
- Sitelist.xml
- McAfee Agent Log Files
- Using Log Files
- Installation Folders
- Check Your Understanding
- Lab Exercises

Module 5: Overview of Encryption Technologies and Computer Boot Concepts
- Safeguarding Data
- Protection from Data Loss
- Data Privacy Laws
- Safeguarding Data with Encryption
- Difference Between Disk and File Encryption
- Difference Between Disk and File Encryption
- Common Enterprise Requirements
- Check Your Understanding
- Encryption Concepts
- Basics of Encryption
- Importance of Key Length
- Symmetric Keys
- Advanced Encryption Standards
- Key Exchange
- Asymmetric Keys
- Cryptographic Hash Functions
- Authentication Methods
- The Computer Boot Process
- The Computer Boot Process
- Boot Process
- Computer Boot
- Check Your Understanding

Module 6: Introduction to McAfee Drive Encryption
- Drive Encryption Defined
- McAfee Data Protection Portfolio for Endpoint
- Security Features of Drive Encryption
- Check your Understanding
- Drive Encryption Components
- Drive Encryption Overview (from ePO Server)
- Drive Encryption Overview (from Client)
- DE Pre-Boot Environment
- System Boot Sequence – No DE Encryption
- System Boot Sequence – With DE Encryption
- McAfee Drive Encryption
- DE Keys
- DE Tokens
- DE Key Storage
- User Logon Process
- Authentication Security Models for Windows
- GINA Logon Process with DE
- Credential Provider Logon Process with DE
- User Passwords
- Resources
- Check your Understanding

Module 7: Solidcore Client
- Pre-Installation Considerations
- Before Installing DE 7.1
- Pre-Installation Considerations
- Network Considerations – Open Ports
- ePO Server Hardware Requirements
- ePO Software Requirements
- Client Requirements
- Drive Encryption Software
Course Description

- McAfee Download Site
- Supported Tokens and Readers
- Check your Understanding
- Downloading the Software
- DE Installation
- DE Menus
- DE Server Settings
- General and PC Software Settings
- Simple Passwords and Tokens
- Non-compatible Software and Themes
- Theme Modification
- Check your Understanding
- Lab Exercises

Module 8: Active Directory Configuration
- Summary of the Installation Process
- LDAP Authentication
- Active Directory
- Configuration Workflow
- Populating the ePO System Tree with AD
- Registering LDAP Servers in ePO
- Registering LDAP Servers
- Troubleshooting Registered LDAP Servers
- Verifying AD Login in ePO
- Check your Understanding
- Mapping System Tree Structure with AD
- System Tree – Managed Systems
- Synchronizing AD with ePO System Tree
- LDAP Synchronization Task for DE
- LDAP Synchronization for DE
- LDAP Synchronization
- Lab Exercises

Module 9: DE Users
- DE Users
- DE User Menu
- Adding a DE User to a System
- View a DE User Added to a System
- Adding DE Users – Automated
- Blacklist Rule with ALDU
- User Group Inheritance in ePO
- Adding Group Users to Systems
- Deleting a DE User From a System
- Check your Understanding
- Lab Exercises Only

Module 10: Installing DE onto Clients
- Summary of the Installation Process
- DE Client Deployment Process
- Client Requirements Review
- Pre-Installation Considerations Review
- Pre-Installation Considerations
- Pre-Installation – Drive Encryption Go
- Deploying DE Agent and Software
- Verifying EEPC Installation
- Verifying Installation
- Events on the Client
- New Processes on the Client
- System Details After Default Policies Deploy
- Deployment
- Check your Understanding
- Lab Exercises

Module 11: Offline Activation
- Offline Activation Overview
- Offline Activation Walk-Through
- Check your Understanding

Module 12: Drive Encryption Policies
- Summary of the Installation Process
Course Description

- Overview of Policies
- Policy Application and Inheritance
- Check your Understanding
- DE Policies Overview
- DE Product Settings Policy
- User Experience
- User Based Policies
- Enforce UBP Configuration
- Policy Scenario
- Policy Assignment Rule
- Policy Assignment Rule – User Based Example
- Check your Understanding
- Lab Exercises

Module 13: DE Dashboard and Reports
- DE Reports and Queries
- Default Reports
- Example Report Output
- Actionable Reports
- Creating a New Query
- Dashboards
- DE Dashboard and Monitors
- Managing a Dashboard
- Check your Understanding
- Lab Exercises Only

Module 14: DE Administrative Users
- Purpose of Administrative Users
- Automatic Administrative Users in ePO
- Creating Automatic Administrative Users in ePO
- Automatic Administrative Users in ePO
- Permission Sets
- Permission Sets Explained
- Creating a DE Permission Set
- Manually Creating a DE Administrative User
- ePO View with DE Permission Set
- Check your Understanding
- Lab Exercises

Module 15: Troubleshooting DE
- Troubleshooting DE
- Researching the Problem
- Current Known Issues
- Interaction between AntiVirus and DE
- Knowledge Base Articles
- Help Files
- Machine Info Report
- Minimum Escalation Requirements (MER)
- Collect Additional Information
- Log Files for ePO Server
- Enabling Orion.log Debugging
- Restarting SQL Processes on ePO Server
- Log Files for McAfee Agent
- Viewing the Agent Log File
- Debug Logging on the Client
- MfeEpe.log
- DE Error Codes and Messages
- LDAP Synchronization Issue
- Agent Activation Issue
- Check your Understanding
- Lab Exercises

Module 16: Recovery Configuration
- DE Recovery Options
- Traditional Self Recovery Configuration
- Self Recovery of User Password
- Reset Self-Recovery
- Smartphone Self-Recovery
- Administrative Recovery
Course Description

- Administrative Recovery – ePO Administrator
- Check your Understanding
- Lab Exercises Only

Module 17: Disaster Recovery with DETech
- Disaster Recovery Needs and Scenarios
- Requirements for Disaster Recovery
- Capabilities of each Disk Type
- Creating DETech using Bart PE
- EZPE Builder for Data Recovery
- EZPE Builder for Data Recovery
- Windows Assessment and Deployment Kit
- Windows Assessment and Deployment Kit (Video)
- Windows Assessment and Deployment Kit 8.1
- Customize – Start with Phase
- Phase EZPE Builder (Bit)
- Customize – End with Phase
- Make a Bootable USB/CDROM
- EZSA Builder for Data Recovery
- Exporting Recovery Information from ePO
- Check your Understanding
- Booting the EZPE Recovery USB\CD
- Booting EETech Recovery CD
- Operations
- Authorization and Authentication
- ActionsWorkspace
- Emergency Boot
- Decrypting with Remove EE
- Crypt Sectors
- Force Decrypt
- Restore MBR
- Edit Disk Crypt State
- Repair Disk Information
- Set Algorithm
- Set Boot Disk
- Check your Understanding
- Lab Exercises

Module 18: DE Scripting
- Scripting Overview
- Python Client
- ePO Scripting
- DE Scripting
- Check your Understanding
- Lab Exercises

Module 19: Uninstalling DE & Upgrade Overview
- Steps in Uninstall
- Disable DE Policies – For All Systems
- Modify Policy – Break Inheritance
- Modify Policy – On Single System
- View Decryption from Dashboard
- View Policy Update in Agent Monitor
- Decrypted Client System
- Remove DE from Client
- Check your Understanding
- Manually Uninstalling from a Client
- Check your Understanding
- Migration
- End User Experience
- OS Refresh
- Lab Exercises Only

Module 20: Endpoint Assistant
- The Beginning – Starting with the UBP Policy
- Product Settings – Companion Devices
- User Based Policies – Companion Devices
- New System – Register Smartphone
Course Description

- PBFS – Default Password and Logging on
- PBFS – First Time Password Change
- User Password Recovery Questions
- Downloading the Endpoint Assist iPhone
- Scan QR Code with Endpoint Assist
- Endpoint Assistant – The QR Code
- Scenario: I forgot my password!
- Administrator / Smartphone Recovery
- Smartphone time!
- Enter the code into Line
- Enter the code into Line
- Finishing up!
- Troubleshooting – Re-Register your System on EA
- Module 21: McAfee Data Protection Self Service Portal (DPSSP)
- What is the Self Service Portal?
- Important
- Software needed
- Instructions
- Server Settings
- Edit DPSSP Settings