

## McAfee Intranet Defense: VirusScan Enterprise 8.0i and ePolicy Orchestrator 3.5

This course provides extensive hands-on experience in the installation and configuration of McAfee<sup>®</sup> point products that provide intranet anti-virus protection: McAfee VirusScan<sup>®</sup> Enterprise 8.0i and Installation Designer 8.0. Through detailed lab exercises, participants also learn to deploy and manage these products using the McAfee ePolicy Orchestrator<sup>®</sup> (ePO<sup>™</sup>) 3.5 management tool.



### Skill Building

Before taking this class we recommend that participants have a general understanding of viruses and anti-virus technology.

### Exercises

All topics are supported by laboratory exercises specifically designed to increase knowledge retention. Classroom labs provide the basic hands-on experience needed to install, configure, and manage McAfee anti-virus products.

### Course Materials

- Student Manual

### Duration

- Four Days

### Students Learn to

- Install and configure McAfee Installation Designer v 8.0
- Describe the components and features of ePO
- Install ePO 3.5
- Log on to the ePO console, build the directory tree, and deploy software
- Define the ePO Agent and describe its interaction with the ePO Server
- Deploy and manage the ePO Agent
- Deploy and manage VirusScan Enterprise 8.0i via ePO
- Run reports from the ePO reporting database
- Describe how ePO interfaces with Microsoft SQL
- Deploy and manage ePO repositories
- Create a SuperAgent Repository
- Deploy Global Updating and manage global DAT updates
- Add product software updates to ePO
- Create custom queries
- Maintenance of ePO

### Suggested Next Course

To gain a core set of skills and knowledge on anti-virus management, participants may also choose to attend:

- Anti-Virus Administration for GroupShield (TRN-AVD-201-TCL)
- Anti-Virus Administration for WebShield (TRN-AVD-301-TCL)

### Contact Information

Phone: 866-210-2715

E-mail: [education@mcafee.com](mailto:education@mcafee.com)

*Training for McAfee Anti-Virus and Intrusion Prevention Products, including McAfee Enterecept<sup>®</sup> and IntruShield<sup>®</sup>*

## Daily Outline

### Day 1

#### **VirusScan Overview**

- Features and highlights
- Trusted connection strategy
- VirusScan components
- Companion utilities
- The Common Framework

#### **Installation**

- Hardware and software requirements
- Permissions required for installation
- Installation methods and options
- Installation process and uninstall.ini
- Installation on a cluster server
- VirusScan files and directories
- Repair and removal
- *Lab: Installing VirusScan using a GUI*
- *Lab: Installing and removing VirusScan using a command line*

#### **Configuration**

- Accessing VirusScan
- The console
- Default tasks and policies
- Access protection using port blocking
- File, share and folder protection
- Default access protection rules
- Creating rules
- Buffer overflow protection and exclusions
- Unwanted program protection
- On-access scanner configuration
- Scriptscan component
- Scanner exclusions in Microsoft Exchange and Lotus Domino
- Low and high risk process protection
- Testing virus detection
- E-mail scanning on-delivery and on-demand
- On-demand scanner and scheduler configuration
- Scanning from the command line
- User interface and remote administration options
- *Lab: Creating and testing a port blocking rule*
- *Lab: Configuring and testing a file, share and folder protection*
- *Lab: Testing buffer overflow protection*
- *Lab: Testing unwanted program policy*
- *Lab: Identifying default scanner configuration*
- *Lab: Configure high and low risk scanning*
- *Lab: Password protecting the user interface*

#### **Updating**

- Overview
- Types of update
- Signature and engine updates
- Other updates
- Update strategies
- McAfee Web Sites

- Security features in the update process
- Default updating
- The autoupdate task and process
- Incremental updating
- Configuring and scheduling autoupdate
- Editing autoupdate repository list
- Alternative updating methods
- The mirror task and process
- *Lab: Creating an ftp server to host updates*
- *Lab: Mirror from a remote server to a local repository*
- *Lab: Modify the VirusScan repository list*
- *Lab: Configure and schedule an autoupdate package*

### Day 2

#### **Policy and Strategy**

- The challenges faced by enterprises
- Anti-virus policy development
- Compliance, enforcement and visibility
- ePO-managed products
- ePO components and processes

#### **Installation**

- Pre-requisites and environmental factors
- Deployment options
- Server and database sizing
- Upgrade paths to ePO 3.5
- The installation process
- The ePO console and interface
- *Lab: Installing ePO 3.5*
- *Lab: Accessing the ePO Console*

#### **The ePO Agent**

- Installation requirements and supported platforms
- Deploying the agent through the console
- Deploying the agent using scripting
- Other deployment methods
- Understating ePO Agent files
- Customising the agent installation package
- Using the small business wizard
- Accessing agent log files
- Agent communications
- Forcing agent activity
- The SuperAgent
- *Lab: Creating a site for your ePO Agent*
- *Lab: Forcing agent activity*
- *Lab: Viewing agent log files*
- *Lab: Reviewing contents of agent log files*

**Day 3****The Directory**

- Directory concepts
- Directory organisation methods
- Sites, groups and inheritance
- Identifying directory objects
- Methods for creating the directory
- Active directory discovery
- IP address filtering
- Rogue system detection
- ePO Console roles
- *Lab: Using IP filtering*
- *Lab: Examining console account roles*
- *Lab: Using an active directory discovery task*
- *Lab: Using a rogue system detection sensor*

**Policies, Properties and Tasks**

- Policy flow and inheritance
- Policy concepts
- Agent policies and communication
- Agent update options
- Product Policies
- Import and export of policies
- System Compliance Profiler
- Entercept features
- Site, group and machine computer properties
- Client update tasks
- *Lab: Setting agent policy and observing inheritance*
- *Lab: Confirming policy enforcement*
- *Lab: Examining machine properties*
- *Lab: Setting VirusScan policy*
- *Lab: Observing agent event collection*
- *Lab: Adding a VirusScan scan task*

**ePO Server Tasks and Repositories**

- Repositories overview
- Repository pre-requisites and system requirements
- Managing updates
- Mobile computer update options
- Selective updating
- Master and distributed repositories
- Source and fallback repositories
- Creating repositories
- Managing software in a repository
- Tasks types and definitions
- Compliance checking
- Pull and replication tasks
- Repository selection
- Sample topologies
- Global updating
- SuperAgent repository replication
- Notifications
- *Lab: Adding software to the repository*
- *Lab: Deploying VirusScan using ePO*
- *Lab: Creating a pull and replication task*
- *Lab: Using global updating*

**Day 4****ePO Reporting**

- Accessing the ePO database
- Authentication restrictions
- Database options
- Directory filtering
- Event filtering
- Reports types and the report interface
- Infection and coverage reports
- Report drilldown
- Customising reports and saving settings
- Adding reports
- Query types
- Running a query
- Examining queries
- Adding queries
- *Lab: Running ePO reports and queries*
- *Lab: Writing and adding queries*

**Maintenance and Monitoring**

- Server events and performance counters
- Directory operations
- Configuring ePO to SQL authentication
- Backup and Restore
- *Lab: Backup and Restore of database*