

## **IQVelocity Course 1005A: McAfee® Advanced ePO™ 4.0 Advanced and Best Practices**

### **Module 1: Product Management with Policies and Client Tasks**

- What is policy management
  - Working with the Policy Catalog, policies, and client tasks
    - Categories
    - Policy enforcement
    - Exporting and importing
    - Inheritance
    - Assignment
    - Assignment locking
    - Ownership
    - Editing, creating, duplication, renaming, and management of policies
- Client tasks and what they do
  - Update
  - On-demand

### **Module 2: Software Deployment and Updates**

- What are extensions
  - Installing new extensions
- Deployment packages for products and updates
  - Checking in product deployment and update packages manually
    - ZIP files
    - DAT files
    - Patch ordering and dependencies
  - Using the Deployment task to deploy products to managed systems
  - Deploying update packages automatically with global updating
    - Process and requirements
  - Deploying update packages with pull and replication tasks
    - Selective updating
  - Configuring agent policies to use appropriate distributed repository
  - Updating managed systems regularly with a scheduled update task
  - Confirming that clients are using the latest DAT files
  - Replication tasks

### **Module 3: Server Settings and tasks**

- Server settings and chaining
  - Server name and http port for communication
  - email server
  - filtering
  - global updating
  - printing and exporting
  - security keys
  - system tree sorting
- Other server tasks
  - Repository Replication

- Data Rollup
- Purge Event Rollup Records
- Purge Event Logs
- Purge Audit Logs

#### **Module 4: Reporting**

- Queries
  - Default Queries and applicable actions
  - Creating custom queries with the Query Builder
  - Public and private queries
  - View query SQL
- Server Task Log
  - Analyzing logs and purging
- Notification Log
  - Analyzing logs using filters, group type, and display type.
  - Purging logs
- Audit Log
  - Analyzing logs and purging
- Event Log
  - Analyzing logs and purging
- MyAvert

#### **Module 5: Repositories**

- Repository types and what they do
  - Master
    - Check in package options
      - ZIP, DAT, EXE
    - Pull now
    - Schedule pull
    - Configure proxy settings
  - Source
  - Distributed
    - SuperAgent, FTP, HTTP, UNC, Local, mirror
  - Fallback
- Branches
  - Current
  - Evaluation
  - Previous
- Importing and exporting the repository list to a file: Sitelist.xml

#### **Module 6: Notifications**

- How does notifications work
- Throttling and aggregation
- Fine tuning notifications for virus outbreaks
  - Servers
  - Workstations
  - Groups
- Creating and editing Notification rules

- Notification permissions
- Email list
- SNMP server
- External commands
- Filtering
- Thresholds
- Viewing the history of Notifications
- Product and component list

### **Module 7: ePO 4.0: Behind the Scenes**

- ePO server
  - McAfee ePolicy Orchestrator 4.0.0 Application Server
    - "D:\Program Files\McAfee\ePolicy Orchestrator\Server\bin\tomcat5.exe"  
//RS//MCAFEETOMCATSRV
    - Dependencies: MSSQL and NT LM Security Provider
    - Functionality and operations
  - McAfee ePolicy Orchestrator 4.0.0 Event Parser
    - "D:\Program Files\McAfee\ePolicy Orchestrator\EventParser.exe"
    - Dependencies: MSSQL and NT LM Security Provider
    - Functionality and operations
  - McAfee ePolicy Orchestrator 4.0.0 Server
    - "D:\Program Files\McAfee\ePolicy Orchestrator\Apache2\bin\Apache.exe" -k  
runserviceMcAfee security agent (CMA)
    - Dependencies: MSSQL and NT LM Security Provider
    - Functionality and operations
  - <https://172.20.1.2:8443/core/orionSplashScreen.do>
- SQL Server
  - Proper steps in backing up and restoring
  - d:\PROGRA~1\MICROS~1\MSSQL\bin\sqlservr.exe
  - SQL Agent
    - d:\PROGRA~1\MICROS~1\MSSQL\bin\sqlagent.exe
- McAfee Security Agent (CMA)
- Performance counters
  - McAfee Framework Service
    - "C:\Program Files\McAfee\Common Framework\FrameworkService.exe"  
/ServiceStart
    - Dependencies: RPC
- Repositories
- Directory structure
  - D:\Program Files\McAfee\ePolicy Orchestrator\
  - D:\Program Files\McAfee\ePolicy Orchestrator\DB\Audit Logs
  - D:\Program Files\McAfee\ePolicy Orchestrator\DB\Logs
  - D:\Program Files\McAfee\ePolicy Orchestrator\DB\Software
    - ZIP
    - MCS
    - Upd versus gem files
    - Delta.ini, update.ini
    - Replica.log, DATinstall.mcs

- Catalog.z
- DBbak.exe
- Sitelist.xml

**Module 8: SQL Server**

- Enterprise Manager
  - ePO\_computername database
    - Backup options: complete, differential, append, overwrite
    - Setting up a schedule and options
    - Shrink database: D:\Program Files\Microsoft SQL Server\MSSQL\Data\ LDF and MDF files
    - Separate physical drives recommended
    - Tables
    - Maintance
  - Core/config