

**IQVelocity Course 1074A:
McAfee® ePO™ 3.6.1 to 4.5 Upgrade**

Module 1: Architecture and Requirements in ePolicy Orchestrator 4.5

- New Components of ePO
 - ePO Server
 - Tomcat Service
 - Event Parser Service
 - Apache Service
 - McAfee Agent (CMA)
 - SQL Server
 - Repositories
 - Registered Servers
 - Remote Agent Handlers
- Overview of new features in ePO 4.5
 - Scalability
 - Custom Data Channel
 - Improved security for agent-to-server communication
 - Move agents between servers
 - Navigation redesign
 - Drag-and-drop
 - Policy Assignment Rules
 - Automatic Responses
 - IPv6 support
 - Issues and ticketing
 - Multi-server roll up reporting improvements
 - Active Directory improvements
 - Queries system improvements
 - Rogue System Detection improvements
 - Searchable help
- Known Issues
- System, server, database, repositories, SA, and agents for non-Windows environments

Module 2: Prepping ePolicy Orchestrator 3.6.1 for the upgrade

- Steps needed before upgrade
 - Read doc: readme.htm, install.pdf, etc
 - Change agent to server communication port from 80
 - OITunnel.exe and KB article NAI31903
 - Upgrade your network to CMA 3.6 or higher
 - Upgrading to ePO 3.6.0 pr PrP 1.5 patch 1
 - Upgrade to HIPS 7.0
 - Upgrade SCP to 2.0
 - Rogue Sensor module comes out in Q1 of 2007
 - Upgrade all machines to VS 8.0i
 - Remove all events older than x days
 - Remove unused products from repository
 - Remove duplicate computers
 - Remove inactive agents
 - Repair orphaned events
 - Shrink database and log
 - DBBak.exe and Sitelist.xml

- SQL Server Management Studio or 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
- Backing up the database and exporting sitelist.xml
 - DBbak.exe and SQL Server Management Studio
- Difference between SQL and Windows Authentication
- Disable VirusScan and Framework Service until the installation is finished
- Options before installing ePO
 - MSXML 6.0
 - Net Framework 2.0
 - SQL 2005 Server
 - SQL 2005 Server Backward Compatibility

Module 4: Upgrading to ePO 4.5

- Requirements
 - ePO Server requirements
 - Agent Handler requirements
 - Database requirements
 - Distributed repositories requirements
 - Agent and SuperAgent requirements
 - Requirements for agents in non-Windows environments
 - Operating systems language support
- Supported products and components
 - First time installation of the Agent Handlers
- Unsupported products
- Performing backups before upgrading
 - Security Keys
 - <https://<servername>:8443/core/config>
 - SQL Database
- Upgrading the ePO server from version 4.0 – KB51438
 - Needed products and tools
 - Steps in running the upgrade process
- Running ePO 4.5 setup.exe and choosing options
- Entering the license key
 - Verified when attempting to download McAfee content
- Post Installation tasks
 - Verify all services are running and check Event Viewer for any errors
 - Creating and modifying server tasks
 - Checking over policies for all software
 - Redeploying repositories
 - Check in packages
 - Migrate events if necessary
 - Upgrade agents if needed
- Overview of the GUI
 - Menu
 - Reporting
 - Systems
 - Policy

- Software
- Automation
- User management
- Configuration

Module 5: Demo of Implementing New Features in ePO 4.5

- Using the Web 2.0 GUI
 - Navigation redesign
 - Drag-and-drop
- Scalability
 - Agent Handlers
 - ePO without Tomcat service
- Security enchantments
 - TLS improves security for agent-to-server communication
 - 3 Pair of security keys
- Improved Agent Management
 - Automatic new GUID generation with duplicates
 - Custom Data Channel
 - Agent 4.5
 - Instant communication with non-policy data
 - Ex: scan now, update now
- Policy Assignment Rules integrated with Active Directory
- Automatic Responses with support SNMP v1-v3
- IPv6 support
- Issues and ticketing
 - Support Remedy HelpDesk and OpenView Servicedesk
- Multiple ePO Management
 - Sharing of policies
 - Move agents between servers
 - Multi-server roll up reporting improvements
- Active Directory improvements
- Queries system improvements
- Rogue System Detection improvements
- Searchable help

Module 6: Configuring initial ePO Configuration

- Registering LDAP servers for use with ePolicy Orchestrator
- Managing ePO users with Active Directory

Module 7: Reporting

- Dashboard
- Queries
 - My Groups
 - Shared Groups
- MyAvert

Module 8: Automation

- Server Tasks
 - Inactive Agent Cleanup Task for 4.5
 - Update Master Repository FTP and HTTP
 - Active Directory Synchronization/NT Domain
 - Purge Logs

- Repository Replications
- Run Query
- Automatic Response
 - Creating and managing response
- Issues
 - Creating basic issues manually

Module 9: Systems

- The System Tree
 - Systems
 - Create time based password
 - Rogue Sensor
 - Tag
 - Agent
 - Directory Management
 - Ping
 - Wake up agent
 - Assigned Policies
 - My Default
 - Client Tasks
 - Deployment
 - DAT update
 - Engine, Hotfix, SP update
 - On-demand
 - Group Details
 - Creating, deleting, moving groups
 - Deploying agents to group
 - Check IP Integrity
 - Wake up agents
- Considerations when planning your System Tree
 - 2 main reasons: bandwidth control and policy placement
 - Functional, political, etc
 - Subnets, IP ranges, Tags, Active Directory
- Tag Catalog, Tags, and how they work
- Active Directory and NT domain synchronization
- Criteria-based sorting
- How a system is first placed in the System Tree
- Working with tags
- Creating and populating groups
- Moving systems manually within the System Tree
- Transferring systems between ePO servers
- Sorting and test sorting systems

Module 10: Configuration

- Server Settings
 - Dashboards
 - Email Server
 - Event Filtering
 - Event Notification
 - Global Updating
 - License Key
 - MyAvert Security Threats

- Policy Maintenance
- Ports
- Printing and exporting
- Proxy Settings
- Repository Packages
- Security Keys
- Server Certificate
- System Tree Sorting
- User Auto Creation
- Windows Authentication
- Windows Authorization
- Registered Servers
 - ePO 4.5, SNMP, LDAP
- Agent Handlers

Module 11: Software

- Master Repository
 - Current, Evaluation, and Previous branches
- Extensions
 - What are extensions
 - Installing new extensions
 - Updating and keeping up to date with extensions
- Licensing

Module 12: Policy

- Policy Assignment Rules
 - New policy assignment
 - Choosing users, OU, group membership
- Policy management
- Policy application
- Creating Policy Management queries
- Bringing products under management
- Viewing policy information
- Sharing policies among ePO servers
 - How policy assignment rules work