McAfee® VirusScan and ePolicy Orchestrator Administration Course

Intel Security Education Services Administration Course Training

The McAfee® VirusScan and ePolicy Orchestrator Administration course from McAfee Education Services enables attendees to receive in-depth training on the benefits of the centralized management and deployment of McAfee products. Enabling administrators to fully understand the capabilities of their security solution, not only reduces the risks of misconfiguration, but also ensures that an organization gets the maximum protection from installation.

Course Goals

- Plan the deployment.
- Install and configure ePolicy Orchestrator software.
- Set up the ePolicy Orchestrator server.
- Manage users and resources
- Manage network security, policies, and databases.
- Monitor and report on network security status.
- Install and us McAfee Agent.
- Implement VirusScan Enterprise technologies.

Agenda At A Glance

Day 1

- Welcome
- Security Connected and ePO Overview
- Planning a McAfee ePO Deployment
- Installing McAfee ePO
- Managing Permission Sets and Users
- Creating the System Tree
- Using the Tag Catalog

Audience

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

Register Now for Training

(intel) Security Ⓜ

Course Description

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

Module 1: Welcome
- About this course
- Locating Resources
- Lab Environment

Module 2: Security Connected and ePolicy Orchestrator Overview
- Introducing McAfee Security Connected
- Manifestation of Security Connected
- Security Connected Framework
- Integration with Third-Party Products
- Security Connected Solution Platform
- Solution Overview
- New for this Release
- Basic Solution Components
- Web Interface
- Menu Pages
- Customizing the User Interface
- Architecture and Communication
- User Interface
- Functional Process Logic
- Data Storage

Module 3: Planning a McAfee ePolicy Orchestrator Deployment
- Planning Overview
- Server Hardware Estimates
- ePO Server Hardware Requirements
- ePO Server Operating Systems
- Translated Languages
- Microsoft Prerequisite Software
- SQL Server Database Requirements
- Supported Web Browsers
- Virtual Infrastructure Requirements
- Port Requirements

- Deployment Considerations
- Deployment Scenarios
- Configuration
- Storage Area Network (SAN) Devices
- Managing Scalability
- Environmental Factors
- Implementation Process Checklist
- Change Control

Module 4: Installing ePolicy Orchestrator Software
- Platform Requirements
- Communication Ports
- Deployment Guidelines
- Change Control
- Database Sizing
- Managing Scalability
- Environmental Factors
- Planning Your Installation
- Express, Custom, and Cluster Installation Workflows
- SQL Server Installation
- Installing ePO Software
- Post-Installation Tasks
- Logging into ePO for the First Time
- Importing the Root Certificate
- Using Automatic Product Configuration Tool
- Using Guided Configuration
- Viewing/Editing Port Assignments in ePO
- Maintaining the SQL Database
- Purging the Database
- Basic Troubleshooting
- Configuring ePO for Multiple NICs
- Upgrading ePO

Module 5: Managing Permission Sets and User Accounts
- Permission Sets Overview
- Default Permission Sets
- Configuration Guidelines
- Duplicating or Adding Permission Set
- Editing or Deleting Permission Sets
- Exporting All or Importing
- User Account Overview
- Guidelines for Authentication Types
- Creating User Account
- Personal Settings Overview
- Changing Personal Settings
- Editing Default Session Timeout Interval
- Managing Users with AD
- Registering LDAP Server
- Enabling Active Directory User Login
- Mapping Permission Sets

Module 6: Creating and Populating the System Tree
- System Tree Overview
- Planning System Tree: Considerations
- Planning System Tree: Borders
- Planning System Tree: Ways to Build Tree
- Planning System Tree: Agent Install
- Adding Groups Manually
- Importing System Tree Structure
- AD and NT Domain Synchronization Overview
- NT Domains Synchronization Overview
- Synchronizing NT Domains
- Configuring Agent Push Settings
- AD Synchronization Overview

Course Description

- Registering LDAP Server
- Synchronizing AD
- Maintaining Synchronization
- Moving Groups and Systems
- Best Practices

Module 7: Using the Tag Catalog
- Tag Catalog
- Who Can Use Tags?
- Working with Tag Groups
- Adding Tags with New Tag Builder
- Applying and Clearing Tags from Systems
- Excluding Systems from Automatic Tagging
- Viewing Systems Excluded from Tag
- Applying Criteria-based Tags
- Managing Tags

Module 8: Sorting the System Tree
- System Tree Sorting
- How ePO Determines Placement
- Criteria-based Sorting
- How IP Address Filtering Works
- Checking IP Integrity
- Changing the Sort Order
- Initiating Sort Now
- Initiating Test Sort
- Initiating Move Systems

Module 9: McAfee Agent
- Solution Overview
- McAfee Agent and SuperAgent
- Managed Systems
- New This Release
- Planning the Installation or Deployment
- Platform Requirements
- Installation vs. Deployment

- Update vs. Upgrade
- Communications
- Installation Overview
- Agent Deployment Overview
- Pushing Agent
- Deploying Agent
- Using Agent Install Package
- Creating Client-side Download URL
- Using Smart Installer
- Using Windows Login Script
- Using Agent Image (Windows)
- Converting Agent to Managed Mode
- Removing McAfee Agent
- Using the Command-Line for Customization
- Using System Tray Icon
- Viewing Agent Activity Logs

Module 10: System Information
- Systems Tab Overview
- Customizing the Systems Tab
- Choosing Columns
- Filtering Data
- Viewing System Information
- Using System Information Monitors
- Customizing Summary Monitor
- Customizing Properties Monitor
- Customizing Chart Monitor
- Using System Information Tables
- System Properties Tab Overview

Course Description

Module 11: Client Tasks
- Client Tasks Overview
- Using Client Tasks
- Creating Client Task
- Editing Client Task
- Deleting Client Task
- Duplicating Client Task
- Assigning Client Task
- Task Inheritance
- Editing Task to Block Inheritance
- Other Client Tasks
- VirusScan On-Demand Scan Task
- McAfee Agent Statistics Client Task
- McAfee Agent Wakeup (Windows only)
- McAfee Agent: Mirror Repositories (Windows)
- Product Deployment

Module 12: Managing Policies
- Policies Overview
- Policy Catalog
- Duplicating, Creating, and Editing Policy
- Changing the Owner of a Policy
- Exporting and Importing a Policy
- Renaming or Deleting Policy
- Locking Assignment and Enforcement
- Policy Assignment and Enforcement
- Viewing and Resetting Broken Inheritance
- Policy Comparison

Module 13: Deploying Software for Managed Systems
- Acquiring Software Components
- Software Manager
- Using the Software Manager

- Manually Installing Extensions
- Manually Checking in Packages
- Checkpoint: ePO Summary Dashboard
- Product Deployment Overview
- Product Deployment Project
- Creating a Product Deployment Project
- Managing Deployment Projects
- Viewing Details for Product Deployments
- Client Task Catalog
- Product Update Considerations

Module 14: Repositories
- Master Repository
- Source Repositories
- Fallback Site
- Distributed Repositories
- Default Repositories
- Repository Platforms and Roles
- Repository Branches
- Adding Source Site
- Ensuring Access to Source Site
- Enabling or Disabling Fallback Site
- Editing or Deleting Site
- Adding Distributed Repository
- Enabling Folder Sharing
- Creating SuperAgent Distributed Repository
- SuperAgent LazyCaching
- Creating a Hierarchy of SuperAgents
- Agent Relay Capability
- Collecting McAfee Agent Statistics
- Adding Unmanaged or Local Repository
- Permission Sets
- Export and Import

Course Description

Module 15: Product Maintenance with Repositories

- Global Updating Overview
- Requirements for Global Update
- SuperAgent Repositories and Global Updating
- Enabling Global Updating
- CommonUpdater
- AutoUpdate Process
- Incremental Updating
- Update Progress Dialog
- Server Tasks Log
- Drill-down on Log Entries
- Permission Set for Server Tasks
- Updating Repositories
- Creating a Repository Pull Task
- Creating Repository Replication Task
- Pull and Replication Task Guidelines
- Troubleshooting Task Failure

Module 16: Managing Dashboards and Monitors

- Default Dashboards
- Dashboard Actions
- Assigning Dashboard Permissions
- Dashboards Guidelines
- Monitor Guidelines
- Adding, Editing, Removing Monitor
- Dashboards Server Settings
- Specifying Default Dashboards
- Editing Default Dashboard Refresh Interval
- Designing Dashboards
- Performance Optimizer
- Types of Assessments
- Server Assessment Task

Module 17: Working with Queries and Reports

- Queries and Reports Overview
- Working with Queries
- Basic Query Page Controls
- Using Queries as Dashboard Monitors
- Public and Private Queries
- Using the Query Builder
- Default and Actionable Queries
- Using Preconfigured Queries
- Query Groups and Permissions
- Multi-Server Data Roll-up Overview
- Automatic Query Actions
- Exporting Query Results to Other Formats
- Making Personal Queries Public
- Duplicating and Sharing Queries
- Importing Queries
- Working with Reports
- Settings for Print and Export
- Creating and Editing Reports
- Adding Elements to Report
- Configuring Report Elements
- Customizing Report Headers and Footers
- Viewing Report Output
- Moving a Report to Different Group
- Running Reports
- Filtering Events

Module 18: Automatic Responses and Notifications

- How the Automatic Responses Feature Works
- Enabling Default Rules
- Automatic Response Builder
- Configuring Independent Rules
- Preparing Components and Permissions
- Assigning Permissions
- Specifying Email Contacts List
- Configuring Email Server
- Determining Events to Forward
- Configuring Event Interval
- Specifying SNMP Server
- Importing .MIB Files
- Specifying Registered Executables

Module 19: Database Maintenance and Server Utilities

- Maintenance Overview
- Automating Maintenance with Server Tasks
- Editing Permission Sets for Server Task
- Using cron Syntax in Schedule
- Purge Overview
- Purging Data Manually and Automatically
- Purging Records Using Queries
- Editing Event Filtering Settings
- Backup Overview
- Manually Initiating a Backup
- Restore Overview
- Initiating a Restore
- Transaction Log Overview
- Shrinking Transaction Log
- Using Transact-SQL
- Managing Server Settings

Module 20: Disaster Recovery

- Disaster Recovery Overview
- How Disaster Recovery Works
- Using Server Task for Snapshot
- Taking Snapshot from Dashboard
- Identifying Server Snapshot Status
- Determining a Disaster Recovery Plan
- Scenario: Simple Disaster Recovery Plan
- Scenario: Server Clusters
- Scenario: Cold/Hot Spares - One Physical SiteScenario: Cold/Hot Spares - Two Physical Sites
- Recovery Installation Workflow
- Performing Recovery Installation
- Disaster Recovery Best Practices

Module 21: VirusScan Enterprise Overview

- Solution Overview
- Features and Benefits
- Basic Components
- DATs (Signatures)
- Scan Engine
- DAT and Scan Engine Updates
- Artemis and McAfee Labs
- Optional Components
- Planning a VSE Deployment
- Supported Operating Systems
- Supported Language Choices
- Guidelines for Special Installation Cases
- Installation Overview
- Preconfiguring, Deploying, Updating
- Using McAfee Installation Designer
- Using the VirusScan Console
- Testing VirusScan
- VSE Removal Options

Module 22: VirusScan Best Practices – Part 1
- Access Protection Overview
- Configuring Access Protection
- Buffer Overflow Protection Overview
- Configuring Buffer Overflow Protection
- Potentially Unwanted Programs Overview
- Configuring PUPs
- On-Access Scanning Overview
- Configuring On-Access Scanning
- On-Delivery Email Scanner Overview
- Configuring On-Delivery Email Scan Policies
- Quarantine Manager
- Configuring Quarantine Manager Policies
- On-Demand Scanning Overview
- Configuring On-Demand Scan Task
- VirusScan Mirror Task
- Server Tasks
- Monitoring and Analyzing Protection
- Fine-tuning Protection

Module 23: VirusScan Best Practices – Part 2
- Disabling Processes on Enable
- Configuring Scanning of Trusted Installers
- Exclusions Overview
- Adding/Editing Exclusion Items
- Using Wildcard Exclusions Symbols
- Managing Exclusions with Hardware Paths
- Windows File Protection
- McAfee Agent Exclusions
- Defining Low / High-Risk Processes Policies
- Determining Number of Scanning Policies

- Processes You Can Add as Low-Risk
- Configuring System Utilization
- Filtering 1051 and 1059 Events