Certification Guide

Intel Security Certified Product Specialist

McAfee ePolicy Orchestrator (ePO)

Why Get Intel Security Certified?

As technology and security threats continue to evolve, organizations are looking for employees with the most up-to-date certifications on the most current techniques and technologies. In a well cited IDC White Paper, over 70% of IT Managers surveyed felt certifications are valuable for their team and were worth the time and money to maintain. Becoming Intel Security certified distinguishes you from other security professionals and helps validate that you have mastery of the critical skills covered by the certification exams. Earning a certification also your commitment to continued learning and professional growth.

About Intel Security Certification Program

Currently, Intel offers two industry-recognized certifications as part of our Intel Security Certification Program: Intel Security Certified Product Specialist and Intel Security Certified Security Professional.

The Intel Security Certified Product Specialist certifications are designed for candidates who administer a specific McAfee product or suite of products, and have one to three years of experience with that product or product suite. This certification level allows candidates to demonstrate knowledge in the following key product areas:

- Installation
- Configuration
- Management
- Basic architecture and troubleshooting

The Intel Security Certified Security Professional certifications are designed for security practitioners, penetration testers, auditors, consultants, administrators — with one to three years of experience. This certification level allows candidates to demonstrate knowledge in the following high-level assessment areas:

- Profiling and inventorying
- Vulnerability identification
- Vulnerability exploitation
- Expanding influence

About This Guide

This guide is intended to help prepare you for the **Intel Security Certified Security Professional — ePolicy Orchestrator (ePO)** exam. For more information about other certification exams or about the Intel Security Certification program go to **www.mcafee.com** and select **For Enterprise**, **Services**, and then **Education Services**.

Highlights

This guide has been developed as a resource for your preparation to take the Intel Security Certified Product Specialist — ePO Exam (MA0-100). The following information is provided:

- About the Intel Security Certification Program
- Exam details
- Suggested resources for exam preparation
- Knowledge domain topics
- Sample exam items

intel Security

Intel Security Certified Product Specialist — ePolicy Orchestrator (ePO)

This exam validates that the successful candidate has the knowledge and skills necessary to successfully install, configure, and manage a McAfee ePolicy Orchestrator solution. It is intended for security professionals with one to three years of experience using the McAfee ePO product and associated technologies.

Exam Details

- Associated exam: MA0 -100
- Associated Training: McAfee ePolicy Orchestrator Administration (4 days)
- Number of Questions: 115
- Exam Duration: 140 Minutes
- Passing Score: 72%
- Exam Price: $150 USD (Exam prices are subject to change. Please visit the following link for exact pricing: **http://www. pearsonvue.com/intel/index.asp**

Exam Preparation

Suggested preparation for this exam is:

- 4 Days McAfee ePolicy Orchestrator Administration training (**https://mcafee.netexam.com/catalog.html**)
- Minimum of one year using McAfee ePolicy Orchestrator
- Knowledge domains (see later in the guide)
- Sample questions (see later in the guide)

Certificate Registration

Intel Security has partnered with Pearson VUE, the global leader in computer-based testing, to administer our certification program. Pearson VUE makes the certification process easy from start to finish. With over 5,000 global locations, you can conveniently test your knowledge and become Intel Security Certified.

To register for an exam, go to: **http://www.pearsonvue.com/intel/index.asp**

Exam Duration

The Intel Security Certification Program has built in time to include the following actions during an exam challenge at each testing facility:

- Time to answer exam questions
- Time to review instructions and provide comments after completion

Intel Security reserves the right to change the exam content and time requirements at any time. The most accurate means of obtaining this information is to contact the exam delivery provider on the day of your exam challenge. A notification appears on your screen before the exam begins that shows the maximum time allowed for answering the questions in that exam.

Certification Transcripts

Individuals who have passed an Intel Security certification exam are granted access to the Intel Security Certification Program Candidate site. On the site, you will find:

- Your official Intel Security Certification Program transcript and access to the transcript sharing tool
- The ability to download custom certification logos
- Additional information and offers for Intel-certified individuals
- Your contact preferences and profile
- News and promotions

McAfee ePolicy Orchestrator Administration (4 days)

Although formal training is not required prior to the exam, the **McAfee ePolicy Orchestrator Administration** (4 days) course is recommended.

This course provides in-depth training on how to use McAfee ePolicy Orchestrator (ePO). At the end of this course, you will be able to plan a McAfee ePO deployment, deploy ePO within an existing McAfee ePolicy Orchestrator environment, and configure ePO system components. You will also learn how to use ePO to classify, track, protect, and monitor sensitive information.

To register for this course, go to: **https://mcafee.netexam.com/catalog.html**

Practical (Hands-on) Experience

A minimum of one year of experience using McAfee ePO and associated technologies. Recommended hands-on activities include but are not limited to:

- Architecture design
- Installation/upgrade
- Configuration
- Management
- Troubleshooting

Technical ServicePortal

The Technical ServicePortal provides a single point of access to valuable tools and resources, such as:

- Documentation
- Security bulletins
- Technical articles
- Product downloads
- Tools

To access the ServicePortal, go to: **https://support.mcafee.com**

Expert Center Community

The Expert Center is a community for McAfee product users. Here you will find valuable information for your McAfee products, such as

- Instructional videos and whitepapers
- Discussion feeds for experts and other users
- Guidelines to establish baselines, and to harden your IT environment
- Ways to expedite monitoring, response, and remediation processes

To access the Expert Center, go to: **https://community.mcafee.com/community/business/expertcenter**

Exam Knowledge Domains

Server Installation and Configuration

- Installation (e.g., defaults, ports, components, protocols, encryptions, excluding wizard installation)
- Web Console (e.g., browser versions, navigating the UI, cut and paste features, organizing browser)
- User Accounts
- Permissions sets
- Automatic Responses
- ePO Repositories (e.g., source, fallback, superagent, distributed, master)
- Agent Handlers (e.g., installation and rules)
- Menu/Configuration/Server Settings
- Menu/Configuration/Registered Servers

Server Maintenance and Troubleshooting

- Server Maintenance, utilities, and server tasks
- SQL maintenance
- Log Files
- Recovery
- Performance Monitoring
- Health Checks

Product and Policy Management

- Managing Policies (e.g., duplicating, assigning, creating, deleting, exporting, policy catalog)
- Super/Agent Policies
- Configuration of Product policies
- Installing extensions
- Product Maintenance
- Policy Assignment Rules
- Comparisons (e.g., policy and tasks)
- Client Tasks (e.g., creating, scheduling, applying, inheritance)
- Product Deployment

McAfee Agent

- Installation (e.g., image, third party deployment)
- Agent Communication
- Other Features (e.g., relay servers, peer to peer, agent to agent, hierarchial)
- Logging
- Distributed Depositories
- Troubleshooting (e.g., sitelist. xml, duplicate GUID)

System Tree

- Creating the System Tree
- Populating and Sorting the System Tree
- Tags (e.g., tagging on client tasks/properties/system presorting/reports, tag grouping
- System Information
- Rogue Systems Detection

Queries and Reports

- Creating Queries
- Generating Reports
- Dashboards/Monitors
- Audit Logs
- Event Analysis (e.g., threat events, purging, threat analysis)

Sample Exam Items

The following exam items are provided for review. These items are similar in style and content to those referenced in the Intel Security Certified Product Specialist — ePO exam. The answers are provided after the questions.

1. **Which ePO service manages Agent communication?**
   - **A** Event Parser
   - **B** Framework service
   - **C** Tomcat
   - **D** Apache
2. **A registered LDAP server is used with which of the following authentication types?**
   - **A** SQL authentication
   - **B** Windows authentication
   - **C** Certificate based authentication
   - **D** ePO authentication
3. **Which of the following is true regarding Disaster Recovery?**
   - **A** Database administrator rights are required to change the Keystore encryption passphrase.
   - **B** The Keystore encryption passphrase is used to encrypt and decrypt the sensitive information stored in the server.
   - **C** Disaster Recovery is enabled by default for all database types.
   - **D** The previous passphrase is required to change the Keystore encryption passphrase.
4. **Assignment locking prevents:**
   - **A** Changes to the policy at the parent.
   - **B** Changes to client tasks.
   - **C** Changes to inheritance.
   - **D** Changes by users.
5. **What task can be configured to copy the contents of one distributed repository into another?**
   - **A** Firewall Rule
   - **B** Firewall Group
   - **C** Firewall Options
   - **D** Firewall Catalogs
6. **Policies can be imported into ePO using which file type?**
   - **A** CSV
   - **B** PDF
   - **C** HTML
   - **D** XML
7. **If a policy assigned to the "My Organization" group is deleted, what policy is assigned it its place?**
   - **A** McAfee Default
   - **B** Parent Group
   - **C** My Default
   - **D** Global Group
8. **How can an ePolicy Orchestrator administrator manage assets in a network broadcast segment that cannot communicate directly with the ePolicy Orchestrator server?**
   - **A** Enable peer-to-peer communication
   - **B** Convert the agents to super agents
   - **C** Utilize and Agent Deployment URL
   - **D** Configure an agent relay server

9. What is the purpose of installing the McAfee Agent in VDI mode?

- **A** VDI mode is used to avoid duplicate GUIDs in virtual environments with non-persistent virtual machines
- **B** VDI mode prevents the inadvertent installation of point products that are not compatible with virtual clients
- **C** VDI mode is used to store administrative credentials so that the Agent can be reinstalled if the virtual machine is reprovisioned
- **D** VDI mode is used to provide virtual machines on the same cluster as a source to pull updates in order to save bandwidth

10. What important System Tree property simplifies policy and task administration?

- **A** Hierarchy
- **B** Lock Policy
- **C** Inheritance
- **D** Enforcement

11. When configuring Active Directory synchronization, exceptions can be created for which of the following?

- **A** Organizational Units
- **B** Security Groups
- **C** Domain Groups
- **D** Users

12. When a group has four sorting criteria assigned, the system will be placed into the group when it meets how many of the conditions?

- **A** One
- **B** Two
- **C** Three
- **D** Four

Answer Key

1. D
2. B
3. B
4. C
5. B
6. D
7. A
8. D
9. A
10. C
11. A
12. A

Intel Security
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com