Certification Guide

Intel Security Certified Product Specialist

Data Loss Prevention Endpoint (DLPe)

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 — Data Loss Prevention Endpoint (DLPe)** 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 — DLPe Exam (MA0-103). 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 — Data Loss Prevention Endpoint (DLPe)

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

Exam Details

- Associated exam: MA0-103
- Associated Training: McAfee Data Loss Prevention Endpoint Administration (4 days)
- Number of Questions: 60
- Exam Duration: 140 Minutes
- Passing Score: 78%
- 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 Data Loss Prevention Endpoint Administration training (**https://mcafee.netexam.com/catalog.html**)
- Minimum of one year using McAfee DLPe
- 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 Data Loss Prevention Endpoint Administration (4 days)

Although formal training is not required prior to the exam, the **McAfee Data Loss Prevention Endpoint Administration** (4 days) course is recommended.

This course provides in-depth training on how to use McAfee Data Loss Prevention Endpoint (DLPe). At the end of this course, you will be able to plan a McAfee DLPe deployment, deploy DLPe within an existing McAfee ePolicy Orchestrator environment, and configure DLPe system components. You will also learn how to use DLPe 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 DLPe 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

Networking

- Networking technology theory, principles and practices
- Data networking standards and protocols
- LAN and WAN technologies
- Network administration
- Network and routing protocols
- Baseline conditions
- Perimeter security
- Internal network security
- Basic infrastructure
- Sniffing/network monitoring
- TCP/IP and NAT/PAT

Systems

- Client/server technology
- Group policy overview and security templates
- Web permissions and authorization
- Redundancy/fault tolerance/ high availability
- Drive encryption
- System administration
- Virtual environments
- Processors (CPUs)
- Baseline conditions
- System access and navigation
- Multi-server environments
- Operating systems

Applications

- Databases
- Redundancy
- Web protocols
- Baseline conditions

Policies and Procedures

- Permissions, delegation and auditing
- Policies governing user access
- Role permissions
- Systems testing procedures
- Proactive Protection Scan policy
- Network password procedures
- Company security policies
- Device usage policies
- Change control procedures
- Product specific maintenance
- Incident response procedures
- Role specific escalation
- Corporate security controls
- Corporate security strategy
- Device access control

Architecture and Integration Best Practices

- Level of security required
- Problem isolation tools/
- Industry security standard
- Security monitoring

Security Foundation

- Firewall
- Computer viruses, spyware, and
- Network threat prevention technologies
- Spyware protection
- Firewall technologies and
- Heuristic-based protection
- Authentication
- Vulnerabilities and remediation techniques
- Malware incidents
- Internal threats and attacks
- External threats and attacks
- Security protocols
- Cryptography
- Network security policies
- Network access control
- Common threats and vulnerabilities

Operations and Administration

- Password management
- Network and support management tools and procedures
- Patch management
- Security alerts, front-line analysis and escalation
- Intrusion detection systems
- Monitoring tools
- Problem determination
- Incident and issue categorization
- Basic product functions
- Product policy configuration
- Product report generation
- Version controls
- Detailed product functions
- Protected materials

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 — DLPe exam. The answers are provided after the questions.

1. **You want to prevent unauthorized distribution of tagged data. Which DLPe rule type best meets your requirements?**
   - **A** Classification rule
   - **B** Data rule
   - **C** Protection rule
   - **D** Tagging rule
2. **Which of the following are valid actions for managing content that is no longer relevant?**
   - **A** Add content to the evidence folder
   - **B** Add content to the data-at-rest folder
   - **C** Add content to the data-at-motion folder
   - **D** Add content to the whitelist folder
3. **Which of the following DLP components protects removable media and storage devices?**
   - **A** DLP Endpoint Agent
   - **B** DLP Device Control
   - **C** DLP Incident Manager
   - **D** DLP Service WatchDog
4. **To configure the client software for full protection in Safe Mode, set the functionality in the Agent Configuration:**
   - **A** On the Miscellaneous tab
   - **B** On the Security tab
   - **C** On the Advanced Configuration tab
   - **D** On the File Tracking tab
5. **Which of the following steps is necessary to configure the DLP client software for full protection?**
   - **A** Enable On-the-Go protection
   - **B** Enable Safe Mode option
   - **C** Enable Universal protection
   - **D** Enable WatchDog service
6. **To display the McAfee DLP icon in Microsoft Outlook, the Show Release from Quarantine Controls in Outlook option must be enabled in the Agent Configuration:**
   - **A** On the Miscellaneous tab
   - **B** On the Security tab
   - **C** On the Advanced Configuration tab
   - **D** On the File Tracking tab
7. **Which of the following features lets you temporarily suspend of blocking rules?**
   - **A** Agent bypass
   - **B** Master release
   - **C** Override key
   - **D** Quarantine release
8. **Which of the following definitions are turned off (unavailable) in McAfee DLP Device Control software? Select two.**
   - **A** All Removable Storage Devices
   - **B** Content encrypted by McAfee Endpoint Encryption
   - **C** McAfee Encrypted USB
   - **D** Rights Management
   - **E** Web Destinations

9. Which of the following folder paths and names are recommended initially for use as repository folders? Select all that apply.

- **A** c:\dlp_resources\
- **B** c:\dlp_resources\evidence
- **C** c:\dlp_resources\blacklist
- **D** c:\dlp_resources\whitelist

10. Which of the following are characteristics of Dictionary Matching? Select all that apply.

- **A** Case-sensitive
- **B** Can match phrases
- **C** Can match substrings
- **D** Supports UTF-8

Answer Key

1. C
2. D
3. B
4. C
5. B
6. A
7. A
8. D, E
9. A, B, D
10. B, C, D

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