McAfee™
Together is power.

# McAfee Certified Product Specialist

## Data Loss Prevention Endpoint (DLPe)

## Certification Candidate Guide

# About McAfee Certification

The McAfee 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 these key product areas:

- Basic architecture
- Installation
- Configuration
- Management
- Troubleshooting

For more information about other certification exams or about the McAfee Certification program, go to https://www.mcafee.com/us/services/education-services/security-certification-program.aspx

# Why get McAfee 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 McAfee 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 this Guide

This guide is intended to help prepare you for the McAfee Certified Product Specialist exam. This guides covers these topics:

- Exam details
- Exam topics
- Exam preparation resources

# Exam Details

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

| McAfee Data Loss Prevention Endpoint (DLPe) | |
|---|---|
| Product version(s): | 9.3.2 |
| Associated exam | MA0-103 |
| Associated training | 4 Days McAfee Data Loss Prevention Endpoint |
| Number of questions | 60 |
| Exam duration | 140 Minutes |
| Passing score | 78% |
| Exam price | $150 USD<br>Exam prices are subject to change. Please visit the following link for exact pricing: http://www.pearsonvue.com/McAfee/index.asp |

## Recommended experience

A minimum of one year of experience using the McAfee product. Recommended hands-on experience includes:

- Planning
- Design
- Installation
- Configuration
- Operations and management

## Certification exam registration

McAfee 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 McAfee Certified.

To register for your exam, go to: http://www.pearsonvue.com/McAfee/index.asp

## Certification transcripts

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

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

## Communicating your accomplishment

Once certified, you can obtain an Acclaim digital badge to use in email signatures, on social media, and anywhere you want to showcase your skills and accomplishment.

The skills represented by your Acclaim badge are the key to professional growth and opportunity.

With Acclaim's labor market insights, use your badge and its associated skill tags to search for jobs by job title, location, employer, and salary range. And if you find a job you're interested in, you're just a few clicks away from applying.

# Exam Topics

## 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 (CPU)
- Baseline conditions
- System access and navigation
- Multi-server environments
- Operating systems

## Applications

- Databases
- Redundancy
- Web protocols
- Baseline conditions

## Policies and Procedures

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

## Best Practices

- Level of security required
- Backup and recovery
- Security monitoring
- Problem isolation tools/practices
- Industry security standards

## Security Foundation

- Firewall
- Computer viruses, spyware, and malware
- Network threat prevention technologies
- Spyware protection
- Firewall technologies and intrusion prevention
- 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

# Exam Preparation Resources

Suggested resources for exam preparation include:

- Hands on experience; a minimum of one to three years are suggested
- Instructor Led Training and eLearning courses
- Expert Center
- Technical ServicePortal
- Exam topics
- Sample questions

## Product training

Although formal training is not required to successfully pass the exam, you may benefit from self-paced eLearning content and the shared experiences obtained through instructor led training.

To review course content and register for training, go to https://mcafee.netexam.com/catalog.html

## McAfee Expert Center

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

## Business ServicePortal

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

- Documentation
  - Data Loss Prevention Endpoint 9.3.2 Product Guide (PD25063)
- Security bulletins
- Technical articles
- Product downloads
- Tools

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

# Sample Exam Questions

These questions are provided for review. These items are similar in style and content to those referenced in the McAfee Certified Product Specialist 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 suspend of blocking rules temporarily?
   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.


McAfee™
Together is power.