McAfee
Together is power.

McAfee Certified Product Specialist

Security Information and Event Management (SIEM)

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.

Security Information and Event Management (SIEM)	
Product version(s):	9.3.0
Associated exam	MA0-104
Associated training	4 Days McAfee SIEM Administrator
Number of questions	70
Exam duration	140 Minutes
Passing score	62%
Exam price	$150 USD 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
- 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

- Network password procedures
- 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
  - Enterprise Security Manager 9.3.0 Installation Guide (PD24720)
  - Enterprise Security Manager 9.3.0 Product Guide (PD24719)
  - Documentation Correction: Enterprise Security Manager 9.3.0 Product Guide (KB79268)
- 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. Which feature is accessed via the Receiver Properties?
   a. Alarms
   b. Data Source Profiles
   c. Watchlists
   d. Asset Management
2. Default Event Aggregation occurs on which of the following fields?
   a. Signature ID
   b. Username
   c. Destination Port
   d. Source Port
3. Which of the following components make up the functional SIEM stack?
   a. Data Processing
   b. Correlation
   c. Mitigation
   d. Policy Updating
4. Which of the following statements are NOT true concerning Global Threat Intelligence (GTI) Watchlists?
   a. They are comprised of third-party threat advisories.
   b. They are comprised of Watchlists containing suspicious and malicious IP addresses
   c. They are used as a scoring source
   d. They are licensed from McAfee
5. ELM storage pools require what percentage of allocated space for mirroring overhead?
   a. Firewall
   b. Firewall Group
   c. Firewall Options
   d. Firewall Catalogs
6. Specific event and network flow statistics were gathered from a network over a specific 12-hour period.

- Firewall produced 450,000 total events
- Unix Servers produced 62,000 total events
- Web Applications produced 1,200,500 total events
- Routers produced 150,000,000 total flows

   With these statistics in mind, what is the total EPS for the network?
   a. 3,511
   b. 3,472
   c. 3,500
   d. 3,510
7. Which of the following time zones is the default setting for the McAfee Enterprise Security Manager (ESM) system clock?
   a. International Date Line West
   b. Eastern Standard Time
   c. Greenwich Mean Time
   d. Geo-Location

8. While investigating malware, an analyst can narrow the search quickly by using which of the following watchlists in the McAfee SIEM?
    a. Botnet – Control Channel
    b. Malware Detections
    c. GTI Suspicious and Malicious
    d. Passive DNS – Malware Domain
9. Which of the following statements about Child Data Sources is NOT true?
    a. They will have VIPS, policy and Agent rights
    b. They will be displayed on the Receiver Properties > Data Sources table
    c. They will appear on the System Navigation tree
    d. They do not count towards the total number of data sources
10. Which of the following appliances contains an event database?
    a. ESM
    b. ADM
    c. ELM
    d. DEM

Answer Key

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


McAfee™
Together is power.