McAfee
Together is power.

McAfee Certified Product Specialist

Advanced Threat Defense (ATD)

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 Advanced Threat Defense (ATD)	
Product version(s):	3.6.0
Associated exam	MA0-106
Associated training	4 Days McAfee Advanced Threat Defense
Number of questions	100
Exam duration	140 Minutes
Passing score	67%
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 technology
- TCP/IP
- Network protocols
- Baseline conditions
- Perimeter security
- Internal network security
- Basic infrastructure
- Sniffing/network monitoring
- NAT/PAT

Systems

- Client/server technology
- Group policy security settings
- Web permissions and authorization
- Redundancy/ fault tolerance / high availability
- System administration
- Replication
- Failover
- Virtual environments
- Script writing
- Processors (CPU)
- Baseline conditions
- System access and navigation
- Product specific components
- Multi-server environments
- Operating systems

Applications

- Databases
- Web applications and FTP
- Redundancy
- Web protocols
- Baseline conditions
- Information contained in applications & databases

Policies and Procedures

- Permissions, delegation & auditing
- Role permissions
- Systems testing procedures
- Endpoint protection policies
- Antivirus and antispyware protection policies
- Company security policies
- Change control procedures
- Product specific maintenance procedures
- Incident response procedures
- Role specific escalation procedures
- Corporate security strategy
- Device access control

Architecture and Integration

- Enterprise architecture
- Topology

Best Practices

- Level of security required
- Network management standards
- Comparative product analysis
- Security awareness
- Security monitoring
- Problem isolation tools/practices

Security Foundation

- Web authentication and SSL encryption
- Computer viruses, spyware, and malware
- Network threat prevention technologies
- Authentication
- Vulnerabilities and remediation techniques
- Malware incidents
- Internal threats and attacks
- External threats and attacks
- Security protocols
- Endpoint security
- Common threats and vulnerabilities
- Threat modeling
- Risk assessment

Operations and Administration

- Password management
- Domains, administrators, and passwords creation
- Security alerts, front-line analysis and escalation
- Logs and intrusion detection systems
- Audit logs
- Appropriate tools for monitoring
- Problem determination methods
- Incident and issue categorization
- Basic product functions
- Product policy configuration
- Product report generation
- Version controls
- Detailed product functions
- Product optimization and tuning

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
  - Advanced Threat Defense 3.6.0 Product Guide (PD26471)
- 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 of the following logs can be viewed to determine if the VMDK conversion was successful?
   a. VMDK conversion log
   b. Image conversion log
   c. Validation log
   d. System log
2. An ATD administrator wants to know the maximum supported size for a specific file type. Which of the following commands should the administrator run on the ATD appliance to find out?
   a. show maxsize
   b. Host IPS Content Server
   c. show supported type
   d. Show filetypesize
3. Which of the following will show in the Threat Analysis report if McAfee Active Response identifies hots infected with malware?
   a. Name; infected file(s); operating system of the infected host
   b. Name; infection time; operating system of the infected host
   c. Name; IP; operating system of the identified host
   d. Name; domain; operating system of the infected host
4. In Which of the following locations can an ATD administrator view status of the samples being analyzed?
   a. Analysis | Sample Queue
   b. Analysis | Analyzer Position
   c. Analysis | Analysis Status
   d. Analysis | File Analysis
5. Which of the following is the default time frame for the Analysis Status page?
   a. 24 hours.
   b. 48 hours.
   c. 72 hours
   d. 96 hours
6. Which of the following percentages represents the amount of ATD data disk space that is full when old reports are deleted?
   a. 75%
   b. 80%
   c. 85%
   d. 90%
7. Which of the following dashboards lists the MOST severe malware files in a network?
   a. Top 10 File Types by Name
   b. Top 10 Malware by Threat Name Group
   c. Top 5 URLs Analyzed by GTI
   d. Top 10 Files Types by Volume

8. Which of the following is the default number of user records?
   a. Two
   b. Three
   c. Four
   d. Five
9. A security analyst is verifying that ATD is being backed up regularly as part of a weekly health check. In which of the following ways can the last backup timestamp be located using the ATD web interface?
   a. Click the Manage icon → Backup & Restore → Backup peer-to-peer communication
   b. Click the Manage icon → Logs → System
   c. Click the Manage icon → Backup & Restore → Restore
   d. Click the Manage icon → Logs → Audit
10. On the Point Products monitor display, a yellow "status" for NSP, NGFW, MEG, and/or TIE indicates:
   a. The corresponding product has not submitted a sample in the past 30 minutes.
   b. The corresponding product is sending too many files to ATD in a short time period.
   c. The corresponding product is not communicating with ATD.
   d. The corresponding product has not communicated with ATD in the last 15 minutes.

Answer Key

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


McAfee™
Together is power.