McAfee™
Together is power.

McAfee Certified Product Specialist

McAfee Endpoint Security (ENS)

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 your 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 Endpoint Security (ENS)	
Product version(s):	10.5.0
Associated exam	MA0-107
Associated training	Endpoint Security 10.5
Number of questions	70
Exam duration	140 Minutes
Passing score	66%
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

Endpoint Security Core Settings and Platform Fundamentals

- Install and Configure ENS
  - Installation designer
  - EPO installation
  - Client-side installation
  - Supported platforms
  - Planning the installation
  - Installation outcomes
- ENS Security Modules
  - Updatable content
  - Core features of AMcore
- Configure ENS Policy
  - Client logging
  - Client interface language
  - Common policies
  - Proxy server for McAfee reputation
  - Update configurations
  - Client task/schedule/scan on other modules

Endpoint Security Threat Prevention

- Configure on demand scanning
  - Scan locations
  - GTI
  - Exclusions
  - Actions
  - Scheduling frequency
  - System impact
  - Quarantine
- On Access Protection
  - GTI
  - Process settings
  - Actions
  - Low/high risk processes
  - Default risk processes
  - Default settings
  - Script scan
  - Quarantine
  - Unwanted programs
- Configure ENS Exploit Prevention
  - Exploit prevention policies
  - Protection level Window Data
  - Execution
  - Actions
  - Exclusions
- For Access Protection
  - Process
  - Folder / File name / Path
  - Wild card
  - MD5 hash
  - User defined
  - McAfee defined
  - File/folder based
  - Network port based

Endpoint Security Firewall

- Configure Firewall Rules
  - Location-based rules
  - Time-based rules
  - Rule components
  - Firewall logging
  - GTI
  - Firewall catalog
- Configure Firewall Options
  - Stateful filtering
  - Protection options
  - Trusted executables
  - Defined network
  - Adaptive mode
  - Tuning options
  - Status controls
  - DNS blocking

Adaptive Threat Protection

- Identify Threat Intelligence
  - Threat intelligence
  - DAC Exclusions
  - Processes and workflow
  - Rule sets
- Dynamic App Containment
  - Containment rules/exclusions
  - Observe vs. Enforcement
- Real Protect Scanning
  - Real Protect Cloud-Based
  - Real Protect Client-Based

Endpoint Security Web Control

- Configure Web control settings
  - Block/allow list
  - Content actions
  - Browser control
  - Enforcement messaging
  - Options
- Policy Enforcement
  - Rated sites
  - Customized
  - Site reports
  - Tuning

Endpoint Security Monitoring and Reporting

- Logging
  - Installation logging
  - Log file types
  - Level of logging
- Events
  - On-demand scan events
  - Detection events
  - Threat behavior
  - Threat event origins
- Monitoring Operation and Compliance
  - Content update
  - Repository usage
  - DATs and patch versions
  - Automation
  - Reports and queries

Endpoint Security Migration

- Migration Tasks
  - Setup / pre-migration
  - Automatic vs. manual
  - Local vs. server settings
- Migration Best Practices
  - Assignments
  - Module migration settings
  - Legacy products
  - Migration path
  - Threat prevention
  - Firewall
  - Web control

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
  - Endpoint Security 10.5 Product Guide (PD26799)
  - Endpoint Security 10.5.0 Installation Guide (PD26800)
- 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. When an unknown file is discovered by Adaptive Threat Protection, which of the following is the correct order of processes that the file hash is evaluated?
   a. McAfee GTI, TIE Server, Local Reputation Cache
   b. TIE Server, McAfee GTI, Local Reputation Cache
   c. TIE Server, Local Reputation Cache, McAfee GTI
   d. Local Reputation Cache; TIE Server, McAfee GTI Assignment locking prevents:
2. An ePO administrator has deployed Web Control to the environment, but has not configured any of the settings. Which of the following actions would, by default, happen if a user accesses a site that has not been rated by McAfee?
   a. The user will be allowed to access the site with no notifications.
   b. The user will be prompted to enter an explanation for why they want to see the site.
   c. The user will be blocked from accessing the unknown site.
   d. The user will see a warning message will appear first, then access will be granted. What task can be configured to copy the contents of one distributed repository into another?
3. Which of the following is true regarding Disaster Recovery?
   a. Admin added
   b. User added
   c. Adaptive added
   d. Learning added
4. The incident response team would like to block bittorrent.exe, but allow it to run from an authorized location on Windows systems. Which of the following will meet this requirement?
   a. Within the Threat Prevention Options policy, add the executable to the Potentially Unwanted Program Detections, and add the excluded path within the low-risk exclusion section of the policy.
   b. Select “All Files” within the “What to Scan” section of the Threat Prevention On-Access Scan policy, and then include the allowed path to the exclusions section of the policy.
   c. Add the executable as a high-risk process within the Threat Prevention On-Access Scan policy, and then include the allowed path within the high-risk exclusions section of the policy.
   d. Configure a file or folder path that includes the specified process within the Threat Prevention On-Demand Scan policy, and add the authorized path to the exclusions section of the policy.

Answer Key

1:D, 2:A, 3:B, 4:A


McAfee™
Together is power.