McAfee
Together is power.

McAfee Certified Product Specialist

McAfee Host Intrusion Prevention System (HIPS)

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 Host Intrusion Prevention System (HIPS)	
Product version(s):	8.0
Associated exam	MA0-102
Associated training	4 Days McAfee Host Intrusion Prevention System
Number of questions	115
Exam duration	140 Minutes
Passing score	73%
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

HIP Extension Configuration & Application Maintenance

- Installation (e.g. extension installation, maintenance, upgrade on the server; adding packages; License extension)
- Policy migration
- Property Translator/Catalog Maintenance Server Task (e.g. hidden vs public tasks)
- Updating HIP content (e.g. repository basics; update frequency and size; what, when, why, where; client update task)
- Monitoring and reporting (e.g. dashboards; queries)

HIP Client Configuration and Installation

- Client Installation (e.g. troubleshooting; prerequisites; compatibility)
- User interface/activity log (e.g. packet size and location)
- Command line tools (e.g. client control; FW Info)
- Logs and troubleshooting (e.g. location and type of client log)
- Process file names and functionality
- Linux and Solaris command lines

General Policies

- Client UI policy (e.g. visibility; password/access; client rules)
- Trusted Applications policy (e.g. McAfee default vs custom; effective policy)
- Trusted Networks policy (e.g. options; how they affect other policies; why)

IPS Policies

- IPS Rules policies (e.g. McAfee default vs custom; effective policy; exceptions; application protection; custom signatures)
- IPS Protection policies (e.g. severities and reactions)
- IPS Options policies (e.g. on vs adaptive mode)

Firewall Policies

- Firewall Options policies (e.g. learning vs adaptive mode; startup protection)
- DNS Policies (e.g. wild cards; resolution)
- Firewall Rules policies (e.g. location aware; rule precedents; rule groups; catalog)

Events and Tuning

- Host IPS events (e.g. managing IPS client rules and firewall client rules; threat event log; host IPS event tool)
- Policy tuning (e.g. exceptions; firewall rules)

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
  - Host Intrusion Prevention 8.0 Product Guide (PD22894)
  - Host Intrusion Prevention 8.0 Installation Guide (PD22891)
- 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 preconfigured server task is used to clean up all the adaptive mode rules and catalog entries in the database?
   a. Host IPS 8.0 Catalog Maintenance Task
   b. Duplicate Agent GUID - clear error count
   c. Roll Up Data (Local ePO Server)
   d. Host IPS 8.0 Adaptive - clear error count
2. Which task provides signature updates to HIPs clients?
   a. McAfee Agent Update
   b. Host IPS Content Server
   c. Host IPS Content Server
   d. Repository Pull
3. What is the name of the log in which the ClientControl.exe Utility records its activities?
   a. CC.log
   b. ClientUtility.log
   c. Client.log
   d. ClientControl.log
4. MaxFwLogSize registry key controls the size of:
   a. FireSvc.log
   b. Shield.db
   c. FireEpo.log
   d. Except.db
5. The Connection Isolation option is available for which of the following?
   a. Firewall Rule
   b. Firewall Group
   c. Firewall Options
   d. Firewall Catalogs
6. Which of the following is the command-line troubleshooting tool used for HIPS non-Windows platforms?
   a. fwinfo
   b. hipts
   c. s99hip
   d. clientcontrol
7. Which of the following can be configured on the Client UI policy for non-Windows clients?
   a. Icon display settings
   b. Password for administrative access
   c. Intrusion event reactions
   d. Policy inheritance
8. The Trusted Networks preconfigured default policies:
   a. Includes a list of network addresses automatically.
   b. Can be viewed, edited and exported by the Global Administrator.
   c. Can be applied to Windows and Linux systems.
   d. Includes local subnets automatically.

9. Which signature type can be contained within an IPS Rules Policy?
   a. Host
   b. Digital
   c. Custom Digital
   d. Custom Network

10. Host IPS Firewall rules are found in the:
   a. Host IPS Firewall Rules Catalog.
   b. Host IPS Firewall Catalog.
   c. Host IPS Rules Catalog.
   d. Host IPS Catalog.

Answer Key

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


McAfee™
Together is power.