Certification Guide

Intel Security Certified Product Specialist

McAfee Host Intrusion Prevention System (HIPS)

Why Get Intel Security 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 Intel Security 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 Intel Security Certification Program

Currently, Intel offers two industry-recognized certifications as part of our Intel Security Certification Program: Intel Security Certified Product Specialist and Intel Security Certified Security Professional.

The Intel Security 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 the following key product areas:

- Installation
- Configuration
- Management
- Basic architecture and troubleshooting

The Intel Security Certified Security Professional certifications are designed for security practitioners, penetration testers, auditors, consultants, administrators — with one to three years of experience. This certification level allows candidates to demonstrate knowledge in the following high-level assessment areas:

- Profiling and inventorying
- Vulnerability identification
- Vulnerability exploitation
- Expanding influence

About This Guide

This guide is intended to help prepare you for the **Intel Security Certified Security Professional — Host Intrusion Prevention System (HIPS)** exam. For more information about other certification exams or about the Intel Security Certification program go to **www.mcafee.com** and select **For Enterprise**, **Services**, and then **Education Services**.

Highlights

This guide has been developed as a resource for your preparation to take the Intel Security Certified Product Specialist — HIPS Exam (MA0-102). The following information is provided:

- About the Intel Security Certification Program
- Exam details
- Suggested resources for exam preparation
- Knowledge domain topics
- Sample exam items

intel Security

Intel Security Certified Product Specialist — Host Intrusion Prevention System (HIPS)

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

Exam Details

- Associated exam: MA0-102
- Associated Training: McAfee Host Intrusion Prevention System Administration (4 days)
- 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/intel/index.asp**

Exam Preparation

Suggested preparation for this exam is:

- 4 Days McAfee Host Intrusion Prevention System Administration training (**https://mcafee.netexam.com/catalog.html**)
- Minimum of one year using McAfee HIPS
- Knowledge domains (see later in the guide)
- Sample questions (see later in the guide)

Certificate Registration

Intel Security 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 Intel Security Certified.

To register for an exam, go to: **http://www.pearsonvue.com/intel/index.asp**

Exam Duration

The Intel Security Certification Program has built in time to include the following actions during an exam challenge at each testing facility:

- Time to answer exam questions
- Time to review instructions and provide comments after completion

Intel Security reserves the right to change the exam content and time requirements at any time. The most accurate means of obtaining this information is to contact the exam delivery provider on the day of your exam challenge. A notification appears on your screen before the exam begins that shows the maximum time allowed for answering the questions in that exam.

Certification Transcripts

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

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

McAfee Host Intrusion Prevention System Administration (4 days)

Although formal training is not required prior to the exam, the **McAfee Host Intrusion Prevention System Administration** (4 days) course is recommended.

This course provides in-depth training on how to use McAfee Host Intrusion Prevention System (HIPS). At the end of this course, you will be able to plan a McAfee HIPS deployment, deploy HIPS within an existing McAfee ePolicy Orchestrator environment, and configure HIPS system components. You will also learn how to use HIPS to classify, track, protect, and monitor sensitive information.

To register for this course, go to: **https://mcafee.netexam.com/catalog.html**

Practical (Hands-on) Experience

A minimum of one year of experience using McAfee HIPS and associated technologies. Recommended hands-on activities include but are not limited to:

- Architecture design
- Installation/upgrade
- Configuration
- Management
- Troubleshooting

Technical ServicePortal

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

- Documentation
- Security bulletins
- Technical articles
- Product downloads
- Tools

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

Expert Center Community

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**

Exam Knowledge Domains

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

Firewall Policies

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

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)

Sample Exam Items

The following exam items are provided for review. These items are similar in style and content to those referenced in the Intel Security Certified Product Specialist — HIPS 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** Distributed Repository
   - **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

Intel Security
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com