Certification Guide

Intel Security Certified Product Specialist

Advanced Threat Defense - ATD

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 — Advanced Threat Defense (ATD)** exam. For more information about other certification exams or about the Intel Security Certification program go to **https://www.mcafee.com/us/services/education-services/security-certification-program.aspx**

Highlights

This guide has been developed as a resource for your preparation to take the Intel Security Certified Product Specialist — ATD Exam (MA0-106). The following information is provided:

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

McAfee by Intel

Certification Guide

Intel Security Certified Product Specialist — Advanced Threat Defense (ATD)

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

Exam Details

- Associated exam: MA0-106
- Associated Training: 4 Days McAfee Advanced Threat Administration
- 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/intel/index.asp**)

Exam Preparation

Suggested preparation for this exam is:

- 4 Days McAfee Advanced Threat Administration training (**https://mcafee.netexam.com/catalog.html**)
- Minimum of one year using McAfee ATD
- 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 by Intel

Course Description

McAfee Advanced Threat Defense Administration (4 days)

Although formal training is not required prior to the exam, the **McAfee Advanced Threat Defense Administration** (4 days) course is recommended.

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

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

Recommended Experience and Resources

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

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

Resources

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

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

Exam Knowledge Domains

Monitor/Report/Incident analysis

- Monitor the condition of the environment
  - Endpoint security products (e.g. anti-virus, data loss prevention tools, desktop firewalls, host-based intrusion prevention systems, etc)
  - Daily Monitors: Alerts and Aberrations
- Isolate and troubleshoot problems affecting the condition of the environment
- Monitor potential Information Security events
- Investigate potential Information Security events
- Report on information security events
- Monitor attempted efforts to compromise security protocols
- Interpret vulnerability assessments to gauge strength of security
- Verify events such as perimeter intrusions and breaches in security defenses
- Analyze information assurance security incidents and patterns to determine remedial actions to correct vulnerabilities
- Examine potential security violations to determine if the network environment policy has been breached, assess the impact, and preserve evidence
- Evaluate potential Information Security events as false/positives
- Conduct systems performance monitoring
- Recognize a potential security violation, take appropriate action to report the incident as required by regulation, and mitigate any adverse impact

Operate/Maintain

- Apply security policy and rules as needed
- Administer security policies to control access to systems
- Maintain security endpoint
- Maintain security solution documentation
- Implement vulnerability countermeasures for the enclave
- Write and maintain scripts required to ensure security of the enclave environment
- Manage accounts and access to the ATD environment
- Write and maintain Yara rules for the ATD environment
- Demonstrate proficiency in applying security requirements to an operating system for the network environment or computing environment used in their current position
- Configure ATD
- Maintain ATD: Review automated system maintenance procedures at regular intervals
- Apply instructions and pre-established guidelines to perform information assurance tasks within computing environment
- Apply computing environment specific information assurance program requirements to identify areas of weakness
- Apply appropriate computing environment access controls
- Enter assets in a vulnerability management system
- Implement policy
- 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

Install/Upgrade/Customize/Integrate

- Perform information assurance related customer support functions including installation, configuration, troubleshooting, customer assistance, and/or training, in response to customer requirements for the network environment
- Install ATD appliances
- Customize ATD installation (roles, access, logon banner, SNMP, NTP, DNS)
- Create VMDKs

- Install VM analyzers
- Create profiles (VM and analyzer)
- Perform ATD Maintenance
  - Install, test, maintain, and upgrade network operating systems software and hardware to comply with information assurance requirements
  - Implement applicable patches including IA vulnerability alerts, IA vulnerability bulletins, and technical advisories for their network environment
  - Resolve security product issues
- Upgrade hardware/software
  - Major releases vs. minor releases
  - Upgrade to provide additional capacity
- Given customer requirements, integrate ATD with supported Intel Security / McAfee solutions

Test/Evaluate

- Verify the VM configuration for functionality with ATD: Verify samples are executing properly
- Conduct tests of information assurance safeguards using gold image VMs in accordance with established test plans and procedures
- Evaluate functional operation and performance in light of test results and make recommendations in regards to endpoint updates

Recover/Remediate

- Recommend, schedule, and/or implement information assurance related repairs within the enclave environment
- Use ATD to remediate Information Security events
- Implement response actions in reaction to security incidents
- Analyze and interpret security events for remediation
- Implement technical vulnerability corrections
- Given a set of requirements, design the appliance recovery and disaster recovery plans.

Optimize and Ongoing Analysis

- Analyze ATD environment (appliance/analyzer VMs) for optimal operations and performance
- Analyze existing security controls to protect network resources and ensure compliance
- Evaluate/assess existing monitoring and intrusion response policy configuration
- Analyze user requirements, procedures, and problems

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 — ATD 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 hosts infected with the 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 the 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
   - **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
   - **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

McAfee by Intel

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

Answer key

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

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