CrowdStrike University

CROWDSTRIKE

CROWDSTRIKE UNIVERSITY

CCFA CERTIFICATION EXAM GUIDE

DESCRIPTION

The CrowdStrike Certified Falcon Administrator (CCFA) exam is the final step toward the completion of CCFA certification. This exam evaluates a candidate's knowledge, skills and abilities to manage various components of the CrowdStrike Falcon® platform on a daily basis, including sensor installation.

A successful CrowdStrike Certified Falcon Administrator:

- Understands user management and role-based permissions
- Deploys and manages Falcon sensors and creates groups
- Configures deployment and prevention policy settings
- Configures allowlists and blocklists
- Configures exclusions
- Conducts administrative reporting

CROWDSTRIKE CERTIFICATION PROGRAM

REQUIREMENTS

All exam registrants must (no exceptions):

- Accept the **CrowdStrike Certification Exam Agreement**
- Be at least 18 years of age
- Purchase a CrowdStrike exam voucher

Contact your CrowdStrike Account Executive to request a quote or purchase a CrowdStrike exam voucher through Pearson VUE.

UNIVERSITY SUBSCRIPTION

It is **strongly suggested** that all exam registrants have an active subscription to CrowdStrike University and have confirmed access to their CrowdStrike University account.

- CrowdStrike certification-aligned courses are available to learners with an active CrowdStrike University account.
- A unique CrowdStrike Certification ID, training transcripts and printable certification documents are available through CrowdStrike University learning management system.

NOTE: All exam takers can view and print their CrowdStrike certification exam score report through Pearson VUE.

REQUIRED CERTIFICATION CANDIDATE COMPETENCE AND ABILITIES

- Candidates should have at least six (6) months of experience with CrowdStrike Falcon in a production environment.
- Candidates should read English with sufficient accuracy and fluency to support comprehension. Exams are suitable for non-native English speakers.

ABOUT THE EXAM

ASSESSMENT METHOD

The CCFA exam is a 90-minute, 60-question assessment. Exam questions have been specifically written in a way that eliminates tricky wording, double negatives, and/or fill-in-the-blank type questions. This exam passed several rounds of editing by both technical and non-technical experts and has been tested by a wide variety of candidates.

INITIAL CERTIFICATION

To be eligible for certification, candidates must:

- Achieve passing score on the CCFA certification exam
- Refrain from any misconduct

In the event of misconduct by the candidate, CrowdStrike may invalidate the score and consider any suspicious action a violation of the **CrowdStrike Certification Exam Agreement**.

When a candidate has completed the exam and the candidate's official exam score has been posted, the certification candidate may view the official exam score at Pearson VUE.

RETAKE POLICY

Candidates who do not pass an exam on their first (1st) attempt:

- Must wait 48 hours to retake the exam (wait time begins after the exam)
- Should review the exam objectives, training course materials and associated recommended reading listed in this document.

After the second (2nd) attempt, a candidate will need to wait seven (7) days for the third (3rd) attempt and any subsequent attempts. Wait time begins the day after the attempt.

Candidates that want to retake the exam should consider re-sitting the applicable recommended course(s) and gain additional experience with CrowdStrike Falcon before trying again.

Retakes beyond the fourth (4th) attempt will be considered on a case-by-case basis. CrowdStrike reserves the right to deny a retake beyond the 4th attempt. If the 4th attempt is a failure due to a technical issue the student can reattempt for a 5th time.

If the student fails for a 4th time due to personal performance, they must wait 30 days and retake the recommended training indicated in the exam guide. CrowdStrike will verify that the candidate has retaken the recommended training in the exam guide and has met with the CS Certification Manager before clearing him or her to register for a 5th exam attempt.

Retaking Previously Passed Exams

Candidates will not be permitted to retake any exam they have previously passed unless directly related to a recertification requirement approved by CrowdStrike.

Beta Exams

Candidates will not be permitted to retake beta exams.

EXAM CHALLENGE

If a certification candidate believes there is an error on an exam or that specific questions on the CCFA exam are invalid, contact certification@crowdstrike.com to request an evaluation of your claim. The certification candidate must submit a claim within three (3) days of taking the exam for it to be considered. CrowdStrike will generally respond to your submission within fifteen (15) business days.

RECERTIFICATION

Certification exams are not tied to product versions. The following lifecycle will apply to recertification moving forward, beginning with the date the certification was issued:

- CrowdStrike Certified Falcon Administrator (CCFA): 3 years
- CrowdStrike Certified Falcon Responder (CCFR): 3 years
- CrowdStrike Certified Falcon Hunter (CCFH): 3 years

EXAM PREPARATION

RECOMMENDED TRAINING

CrowdStrike strongly recommends that certification candidates complete these **CSU LP-A: Falcon Administrator Courses** in CrowdStrike University **AND attain six months practical experience** to prepare for the CCFA exam. The courses listed below reflect the current learning path for the CrowdStrike Administration certification:

- CrowdStrike University Orientation
- **FHT 100:** Falcon Platform Architecture Overview
- **FHT 101:** Falcon Platform Technical Fundamentals
- **FHT 102:** Falcon Platform Onboarding Configuration
- **FHT 104:** Activity App Fundamentals
- **FHT 105:** Sensor Installation, Configuration and Troubleshooting
- **FHT 106:** Custom Dashboards
- **FHT 107:** Falcon Firewall Management
- **FHT 121:** Falcon Spotlight Fundamentals
- **FHT 122:** Falcon Discover Fundamentals
- **FHT 160:** Falcon for Mobile
- **FHT 200:** Falcon Platform For Administrators

To learn more about these courses, view the **CrowdStrike Training Catalog**. CrowdStrike also recommends that candidates physically access the Falcon console and perform the exam objectives listed below to prepare for the exam.

RECOMMENDED READING

CrowdStrike strongly recommends certification candidates review the following CrowdStrike Falcon Support Documentation titles to prepare for the CCFA exam:

- Falcon Administration Guides
  - Falcon Console User Guide
  - Users and Roles
  - Customizable Dashboards
  - Falcon Notifications
  - Single Sign-On
- Endpoint Security Guides
  - Start Up and Scale Up
  - Host and Host Group Management
  - Detection and Prevention Policies
  - Real Time Response and Network Containment
  - Device Control
  - Falcon Firewall Management
- Sensor Deployment and Maintenance Guides
  - Falcon Sensor for Windows/Mac/Linux (excluding 5.x for Mac/Container/Mobile/Identity Protection/Home Use/Cloud Workloads)
  - Cloud IP Addresses
  - Sensor Update Policies

EXAM SCOPE

The following topics provide a general guideline for the content likely to be included on the exam; however, other related topics may also appear on any specific delivery of the exam.

1. User Management
2. Sensor Deployment
3. Host Management
4. Group Creation
5. Prevention Policies
6. Custom IOA Rules
7. Sensor Update Policies
8. Quarantine Files
9. IOC Management
10. Containment Policies
11. Exclusions
12. Firewall Policies

13. Falcon Reports
14. USB Policies
15. Real Time Response Policies
16. API Clients and Keys Reporting
17. Notification Workflow

SCOPE CHANGES

In order to better reflect the content of the exam and for clarity purposes, the guidelines below may change at any time without notice. Such changes may include, without limitation, adding or deleting an available CrowdStrike certification, modifying certification requirements, and making changes to recommended training courses, testing objectives, outline and exams, including, without limitation, how and when exam scores are issued. The certification candidate agrees to meet (and continue to meet) the program requirements, as amended, as a condition of obtaining and maintaining the certification.

EXAM OBJECTIVES

The following subtopics and learning objectives provide further guidance on the content and purpose of the exam:

1.0 USER MANAGEMENT

- **1.1** Determine roles required for access to features and functionality in the Falcon console
    - 1.1.1 Describe the capabilities and limitations of each Real Time Response (RTR) role
    - 1.1.2 Create a new user, delete a user and edit a user, etc.

2.0 SENSOR DEPLOYMENT

- **2.1** Analyze the pre-installation OS/networking requirements prior to installing the Falcon sensor
- **2.2** Analyze the default policies and apply best practices in order to prepare workloads for the Falcon sensor
- **2.3** Apply appropriate settings to successfully install a Falcon sensor on Windows, Linux and macOS
    - 2.3.1 Apply basic sensor install requirements and installation processes
    - 2.3.2 Apply additional/advanced options for images/VDI's, tokens and tags
- **2.4** Uninstall a sensor
- **2.5** Troubleshooting
    - 2.5.1 Recognize issues with the basic configuration requirements in the system environment or Falcon components
    - 2.5.2 Resolve policy settings, permissions and threshold issues
    - 2.5.3 Conduct root cause analysis related to system/user issues

3.0 HOST MANAGEMENT

- **3.1** Propose how filtering might be used in the Host Management page
- **3.2** Disable detections for a host
- **3.3** Explain the effect of disabling detections on a host
- **3.4** Explain the impact of reduced functionality mode (RFM) and why it might be caused
- **3.5** Find hosts in RFM
- **3.6** Find inactive sensors
- **3.7** Recall how long inactive sensors are retained in order to define your organization's data backup plan
- **3.8** Determine which reports to use when reporting on information relating to a host
- **3.9** Explain the importance of understanding your company's' Falcon Insight data retention timeframe

4.0 GROUP CREATION

- **4.1** Determine the appropriate group assignment for endpoints and understand how this impacts the application of policies
    - 4.1.2 Describe policy types, components, application and workflow
    - 4.1.3 Define precedence, groups and best practices

5.0 PREVENTION POLICIES

- **5.1** Determine the appropriate prevention policy settings for endpoints and explain how this impacts security posture
    - 5.1.1 Demonstrate what the default policy is used for and apply best practices when configuring default policies
    - 5.1.2 Configure a detection-only policy
    - 5.1.3 Explain what Machine Learning is "on sensor" versus “the cloud”
    - 5.1.4 Describe what each of the different policy setting options do
    - 5.1.5 Define NextGen AV Settings
    - 5.1.6 Describe what End User Notifications do
    - 5.1.7 Assign a prevention policy to groups and hosts
    - 5.1.8 Explain what precedence does regarding prevention policies
    - 5.1.9 Describe policy best practices

6.0 CUSTOM IOA RULES

- **6.1** Create custom IOA rules to monitor behavior that is not fundamentally malicious

7.0 SENSOR UPDATE POLICIES

- **7.1** Determine the appropriate sensor update policy settings and related general settings in order to control the update process
  - 7.1.1 Define an update policy
  - 7.1.2 Demonstrate what the default policy is used for and apply best practices when configuring default policies
  - 7.1.3 Describe what auto-update does
  - 7.1.4 Explain separate policies for MAC/Win/*nix
  - 7.1.5 Explain where build versions are visible for a single sensor or across your environment
  - 7.1.6 Describe what precedence does regarding sensor update policies

8.0 QUARANTINE FILES

- **8.1** Apply options required to manage quarantine files

9.0 IOC MANAGEMENT

- **9.1** Assess IOC settings required for customized security posturing and to manage false positives

10.0 CONTAINMENT POLICY

- **10.1** Configure an allowlist of the appropriate IP addresses, while the network is under containment, based on security workflow requirements
- **10.2** Describe what a containment policy does
- **10.3** Allowlist network traffic so it can connect to contained hosts

11.0 EXCLUSIONS

- **11.1** Interpret business requirement in order to allow trusted activity and resolve false positives and performance issues
  - 11.1.1 Write an effective file exclusion rule using glob syntax
  - 11.1.2 Apply File Pattern Exclusions to groups
  - 11.1.3 Demonstrate how to manage exclusion rules

12.0 FIREWALL POLICIES

- **12.1** Describe how to create a firewall policy
- **12.2** Describe how to configure rule groups, configure traffic rules and apply rule groups to firewall policies

13.0 FALCON REPORTS

- **13.1** Explain the different types of sensor reports and what each report provides
  - 13.1.1 Explain what information is contained in Machine-Learning Prevention Monitoring Report
  - 13.1.2 Explain what information is in the Falcon UI Audit Trail Report
  - 13.1.3 Explain what information is in the API Audit Trail, Prevention Policy Audit Trail, Prevention Hashes Ignored Reports
  - 13.1.4 Explain what information is in the Prevention Policy Debug Report
  - 13.1.5 Explain what information a Linux Sensor Report will provide
  - 13.1.6 Explain what information a Mac Sensor Report will provide
  - 13.1.7 Explain the differences between the Visibility and Hunting reports
  - 13.1.8 Explain the information shown in the Logon Activity Report
  - 13.1.9 Explain the information shown in the Remote Logon Activity Report
  - 13.1.10 Explain the information shown on the Remote Access Graph Report
  - 13.1.11 Explain the information shown on the Geo Location Activity Report
  - 13.1.12 Explain what information can be found in Visibility Reports
  - 13.1.13 Write an effective custom alert rule

14.0 USB POLICIES

- **14.1** Apply a USB device policy to restrict or allow access to USB devices
  - 14.1.1 Create granular device policies
  - 14.1.2 Allowlist and blocklist devices by class, vendor and serial name
  - 14.1.3 Define policies for host groups
  - 14.1.4 Adjust the device control settings
  - 14.1.5 Demonstrate what the default policy is used for and apply best practices when configuring default policies
  - 14.1.6 Describe what precedence does regarding USB device control policies

15.0 REAL TIME RESPONSE POLICY

- **15.1** Apply roles and policy settings, and track and review RTR audit logs in order to manage user activity

16.0 API CLIENTS AND KEYS

- **16.1** Manage API Keys

17.0 NOTIFICATION WORKFLOW

- **17.1** Configure custom alerts to notify individuals about policies, detections and incidents