

CCFA Certification Exam Guide

Description

The CrowdStrike Certified Falcon Administrator (CCFA) exam is the final step toward the completion of the CCFA certification. This exam evaluates a candidate's knowledge, skills and abilities to perform administrative and vulnerability management tasks within the Falcon platform to mitigate and prevent risks.

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 file-path exclusions
- Conducts administrative reporting
- Has at least 6 months experience working in the Falcon platform

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 to register for the exam

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

Learning Access

It is **strongly recommended** that all exam candidates have access to CrowdStrike University and confirm they can view available learning options associated with 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 the CrowdStrike University learning management system.

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

Recommended 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.

Initial Certification

To be eligible for certification, candidates must:

- Achieve a 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 through Pearson.

Retake Policy

Candidates who do not pass an exam on their first 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 attempt, a candidate will need to wait seven (7) days for the third attempt and any subsequent attempts. Wait time begins the day after the attempt.

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

Retakes beyond the fourth attempt will be considered on a case-by-case basis. CrowdStrike reserves the right to deny a retake beyond the fourth attempt. If the fourth attempt is a failure due to a technical issue, the student can reattempt the exam a fifth time.

If the student fails for a fourth 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 CrowdStrike Certification Manager before they are cleared to register for a fifth 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

All CrowdStrike certifications are valid for three (3) years from the date of successful completion of an exam. Recertification requires passing the most current version of the exam upon expiration of certification.

Exam Preparation

Recommended Training

CrowdStrike strongly recommends certification candidates complete the [CrowdStrike Certified Falcon Administrator](#) courses in CrowdStrike University to prepare for the CCFA exam. To learn more about these courses, view the [CrowdStrike Training Catalog](#).

Recommended Reading

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

- Sensor Deployment and Maintenance
- Falcon Management
- Endpoint Security — Response, Configuration and Additional Features sections
- CrowdStrike Marketplace
- CrowdStrike APIs — General Info

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 and Setup
4. Group Creation
5. Policy Application
6. Rule Configuration
7. Dashboards and Reports
8. Workflows

Scope Changes

To better reflect the content of the exam and for clarity purposes, the following guidelines 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. User Management

- 1.1 Determine roles required for access to features and functionality in the Falcon console
- 1.2 Create roles and assign users to roles based on desired permissions
- 1.3 Manage API keys

2. Sensor Deployment

- 2.1 Determine prerequisites to successfully install a Falcon sensor on supported operating systems
- 2.2 Analyze the default policies and apply the best practices to prepare workloads for the Falcon sensor
- 2.3 Uninstall a sensor
- 2.4 Troubleshoot a sensor

3. Host Management and Setup

- 3.1 Understand 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 Locate inactive sensors
- 3.7 Recall how long inactive sensors are retained
- 3.8 Determine relevant reports specific to host management

4. Group Creation

- 4.1 Determine the appropriate group assignment for endpoints and understand how this impacts the application of policies
- 4.2 Apply best practices when managing host groups

5. Policy Application

- 5.1 Determine the appropriate prevention policy settings for endpoints and explain how this impacts security posture
- 5.2 Determine the appropriate sensor update policy settings in order to control the update process
- 5.3 Apply roles and policy settings, and track and review Falcon RTR audit logs in order to manage user activity
- 5.4 Understand the functionality of a containment policy
- 5.5 Configure a containment policy for IP address or subnet exclusions that will apply to network contained hosts based on security workflow requirements
- 5.6 Understand options and requirements to manage quarantined files

6. Rules Configuration

- 6.1 Create custom IOA rules to monitor for behavior that is not fundamentally malicious
- 6.2 Interpret business requirements in order to allow trusted activity, resolve false positives and fix performance issues
- 6.3 Assess IOC settings required for customized security posturing and to manage false positives
- 6.4 Understand configurations for CID wide management within General Settings

7. Dashboards and Reports

- 7.1 Understand the different types of sensor reports and their use cases
- 7.2 Understand the different audit logs and their use cases

8. Workflows

- 8.1 Configure workflows to respond to defined triggers



CROWDSTRIKE

U N I V E R S I T Y

