CROWDSTRIKE UNIVERSITY

CCCS Certification Exam Guide

Description

The CrowdStrike Certified Cloud Specialist (CCCS) exam is the final step toward the completion of CCCS certification. This exam evaluates a candidate's knowledge, skills and abilities to manage various components of the organization's cloud environment and remediate potential threats.

A successful CrowdStrike Certified Cloud Specialist:

- Explains the information and access requirements needed to register cloud accounts, install the Falcon sensors and set up Kubernetes protection
- Determines compliance, rules and policies for cloud security posture management, container security and image assessment
- Registers images in a registry and assesses those images for vulnerabilities
- Configures allowlists and blocklists
- Evaluates cloud security posture, containers and images for misconfigurations and suspicious behavior
- Configures integrations, reports and alerts to operationalize Falcon Cloud Security

CrowdStrike Certification Program

Requirements

All exam registrants must (without exception):

- 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 CCCS exam is a 90-minute, 60-question assessment. Exam questions have been specifically written in a way that eliminates tricky wording and/or double negatives. 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 CCCS 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 24 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 fourth 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 life cycle 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
- CrowdStrike Certified Cloud Specialist (CCCS): 3 years
- CrowdStrike Certified Identity Specialist (CCIS): 3 years

Exam Preparation

Recommended Training

CrowdStrike strongly recommends certification candidates complete the **CSU LP-C: Falcon Cloud Security** courses in CrowdStrike University to prepare for the CCCS 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 CCCS exam:

- Cloud Security Overview
- Cloud Security Posture Management: Cloud Asset Inventory and Visualization
- Cloud Security Posture Management: CSPM Automated Remediation
- Cloud Security Posture Management: Configuring CSPM
- Cloud Security Posture Management: Identity Analyzer
- Cloud Security Posture Management: CSPM Overview
- Cloud Security Posture Management: Monitoring CSPM Assessment Findings
- Cloud Security Posture Management: Troubleshooting Cloud Security Posture Management
- Cloud Security Posture Management: Registering Accounts
- Kubernetes and Containers: Container Security
- Kubernetes and Containers: Kubernetes Protection

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. Falcon Cloud Security Overview and Terminology
2. Cloud Accounts Registration
3. Kubernetes and Container Sensor
4. Falcon Cloud Security Policies and Rules
5. Image Assessment
6. Runtime Protection
7. Reviewing Images
8. Cloud Infrastructure Entitlement Manager (CIEM)/Identity Analyzer
9. Falcon Fusion Workflows
10. Automated Remediations
11. Findings and Detection Analysis
12. Asset Inventory
13. Compliance
14. Dashboards and Reports

Scope Changes

To better reflect the content of the exam and for clarity purposes, the 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:

1.0 Falcon Cloud Security Overview and Terminology

- **1.1** Explain the difference between managed/unmanaged items (like accounts or containers) and assessed/ unassessed items (like container images)
- **1.2** Explain the benefits of Falcon Cloud Security and how all the components work together

2.0 Cloud Accounts Registration

- **2.1** Determine the information and access requirements to register cloud accounts with CrowdStrike Falcon
- **2.2** Create and manage API clients and keys
- **2.3** Register a cloud account with Falcon
- **2.4** Configure a cloud account using APIs
- **2.5** Deprovision cloud accounts from Falcon
- **2.6** Troubleshoot issues related to cloud account registrations
- **2.7** Demonstrate how to set up an assessment schedule for cloud security posture management

3.0 Kubernetes and Container Sensor

- **3.1** Describe the requirements and use of the Kubernetes protection agent
- **3.2** Describe the requirements and use of the Falcon Container sensor in a Kubernetes cluster
- **3.3** Describe the requirements and use of the Falcon sensor on a Linux server
- **3.4** Describe the requirements and use of the Kubernetes Admission Controller
- **3.5** Determine the best sensor to use based on the cloud environment
- **3.6** Troubleshoot issues related to sensor deployment for Kubernetes and containers

4.0 Falcon Cloud Security Policies and Rules

- **4.1** Edit cloud security posture policy configuration settings
- **4.2** Create, edit and delete image assessment policies and exclusions
- **4.3** Create, edit and delete Kubernetes Admission Controller policies
- **4.4** Create, edit and delete Falcon sensor policies
- **4.5** Create custom IOM rules

5.0 Image Assessment

- **5.1** Add CrowdStrike IP addresses to registry allowlists
- **5.2** Demonstrate how to obtain registry credentials from a container registry from the approved registry list
- **5.3** Demonstrate how to register a connection so the image registry can scan images
- **5.4** Demonstrate how to edit and delete registry connection details and settings
- **5.5** Use the Falcon CWPP Image Scanning Script to integrate the Image Assessment tool with the CI/CD pipeline
- **5.6** Describe how to manually scan images using a command-line tool

6.0 Runtime Protection

- **6.1** Find what is running in the environment without deploying a Falcon sensor
- **6.2** Identify unassessed images used in production
- **6.3** Identify IOAs, rogue containers and drift detection
- **6.4** Identify network connections

7.0 Reviewing Images

- **7.1** Identify potential security issues such as malware presence, high-severity CVEs, detected leaked secrets and Docker file misconfigurations from the Image Assessment report
- **7.2** Identify vulnerabilities and installed packages
- **7.3** Identify deployment misconfigurations

8.0 Cloud Infrastructure Entitlement Manager (CIEM)/ Identity Analyzer

- **8.1** Assign policies that determine which users and roles can access particular services
- **8.2** Identify inactive users
- **8.3** Identify the last time a user changed a password
- **8.4** Identify accounts with unnecessary access privileges
- **8.5** Identify accounts that use MFA
- **8.6** Identify accounts that have privilege and don't have MFA
- **8.7** Identify risky Azure Service Principals
- **8.8** Summarize IAM findings and recommend remediations

9.0 Falcon Fusion Workflows

- **9.1** Create custom Falcon Fusion workflows to notify individuals about cloud-related policies, detections, incidents and image assessments

10.0 Automated Remediation

- **10.1** Configure automated remediation workflows for AWS findings
- **10.2** Set up automated remediation within AWS
- **10.3** Explain how to perform an automated remediation dry run

11.0 Findings and Detection Analysis

- **11.1** Evaluate cloud security controls and configurations to identify misconfigurations (IOMs), vulnerabilities and/or high-risk practices
- **11.2** Identify suspicious/malicious activity (IOAs) and associated persistence mechanisms
- **11.3** Explain where to find recommended remediation steps for cloud findings

12.0 Asset Inventory

- **12.1** Identify unmanaged hosts
- **12.2** Identify public assets
- **12.3** Identify risky assets

13.0 Compliance

- **13.1** Compare cloud configurations to the latest industry benchmarks (CIS, PCI, NIST, SOC2) to determine compliance
- **13.2** Create a custom compliance framework

14.0 Dashboards and Reports

- **14.1** Create a scheduled report for IOAs and IOMs