

FALCON 200:

Deploying and Configuring Falcon for Administrators

Course Overview:

Stopping breaches with the CrowdStrike Falcon® platform starts with a robust configuration. To ensure your organization is effectively protected, this comprehensive technical course covers best practice settings for protecting your hosts while advancing your administrative capabilities. Participants will develop proficiency in fundamental aspects of Falcon platform administration, from sensor deployment to advanced configuration settings.

Administrators will develop the expertise needed to implement comprehensive endpoint protection, monitor sensor health, and optimize platform performance. The course emphasizes practical, real-world scenarios that administrators encounter daily, ensuring graduates can immediately apply their knowledge to protect their organizations effectively.

What You Will Learn:

In this course, you will learn how to:

- » Deploy and manage operating system (OS)-specific Falcon sensors in your environment
- » Configure prevention policies, user access, and host groupings
- » Leverage Falcon dashboards and reporting tools to monitor sensor coverage and updates
- » Customize detection capabilities through indicator of compromise (IOC) management and exclusion settings
- » Implement security best practices for enterprise-wide protection

1-day program | 2 credits

This instructor-led course includes various walkthroughs and hands-on learner exercises

Take this class if you are:

A system administrator, a security engineer, or preparing for the CrowdStrike Certified Falcon Administrator (CCFA) exam

Registration:

For a list of scheduled courses and registration access, please log in to your CrowdStrike University account. This course requires two (2) training credits. If you do not have access to CrowdStrike University, need to purchase training credits, or need more information, please contact sales@crowdstrike.com.

Recommended Prerequisites

- » Knowledge of computer networking concepts and protocols, network security methodologies, privacy principles, cyber threats, and vulnerabilities
- » Completion of eLearning courses within the Falcon Administrator Learning Path in CrowdStrike University
- » Familiarity with Microsoft Windows, macOS, and Linux environments
- » Ability to comprehend course curriculum presented in English

Requirements

- » Broadband internet connection, web browser, microphone and speakers
- » Dual monitors and headset are recommended

Class Material

Associated materials may be accessed from CrowdStrike University on the day of class.

Topics

Login and Setup

- » Explore the Falcon console with the credentials provided
- » Determine roles required for access to features and functionality in the Falcon console
- » Create a new user, delete a user, and edit a user

Installation and Configuration

- » Analyze the pre-installation OS/networking requirements prior to installing the Falcon sensor
- » Apply appropriate settings to successfully install a Falcon sensor on Windows, Linux, and macOS
- » Uninstall a sensor
- » Use Host Management to verify sensor properties
- » Explain the different types of sensor reports and what each report provides
- » Recognize issues with the basic configuration requirements in the system environment or Falcon components
- » Determine the appropriate sensor update policy settings and related general settings to control the update process

Host Management

- » Determine the appropriate group assignment for endpoints and understand how this impacts the application of policies
- » Describe policy types, components, applications, and workflows
- » Define precedence, groups, and best practices

Policy Management

- » Determine the appropriate prevention policy settings for endpoints and explain how this impacts security posture
- » Apply options required to manage quarantined files
- » Assess the IOC settings required for customized security posturing and to manage false positives

Threat Management and Exclusions

- » Interpret business requirements to allow trusted activity and resolve false positives and performance issues
- » Write an effective file exclusion rule using glob syntax
- » Apply file pattern exclusions to groups
- » Demonstrate how to manage exclusion rules
- » Create custom indicator of attack (IOA) rules to monitor behavior that is not fundamentally malicious
- » Describe what a containment policy does
- » Based on security workflow requirements, configure an allowlist while the network is under containment with the appropriate IP addresses

