Enterprise Computing Solutions - Education Services

# TRAINING OFFERING

**You can reach us at:**

Arrow ECS, Nidderdale House, Beckwith Knowle, Harrogate, HG3 1SA

Email: educationteam.ecs.uk@arrow.com
Phone: 0870 251 1000

# Check Point Certified Security Administrator (CCSA) and Expert (CCSE) R81.X Boot Camp (includes 180 days' lab access)

| CODE: | LENGTH: | PRICE: |
|---|---|---|
| CKT_CCSAEBC_R81.X | 40 Hours (5 days) | £3,495.00 |

## Description

This 5-day Boot Camp course combines the content of the CCSA and CCSE courses over 5 days (instead of 6).
This course is not for new users to Check Point – previous certification/experience is required.
**Check Point Certified Security Administrator (CCSA)**
The CCSA part of the course covers everything you need to start-up, configure and manage daily operations of R81.10 Check Point Security Gateway and Management Software Blades systems on the GAiA operating system.

**Goals:** Learn basic concepts and develop skills necessary to administer IT security fundamental tasks. **Topics:**

• Security Architecture • Application Control • Deployment • Licensing • Gaia Portal • Hide/Static NAT • URL Filtering • Monitoring States • IoT • Traffic Visibility • Security Events • Threat Emulation • Policy Layers • Browser SmartConsole • Infinity Threat Prevention • User Access

**Check Point Certified Security Expert (CCSE)**
The advanced CCSE part of the course teaches how to build, modify, deploy and troubleshoot the R81.10 Check Point Security Systems on the GAiA operating system.

Hands-on lab exercises teach how to debug firewall processes, optimize VPN performance and upgrade Management Servers.
**Goals:** Validate and enhance your skills and optimally manage Check Point advanced security management systems. **Topics:**
• Management Upgrade and Migration • Management High Availability • Security Gateway Upgrades • Advanced Check Point Maintenance • Security Gateway Operations • Policy Installation • Gaia and Management APIs • Acceleration • Site-to-Site VPN • Remote Access VPN • Mobile Access VPN • Clustering • Advanced Logs and Monitoring

## Objectives

**Check Point Certified Security Administrator (CCSA)**
• Know how to perform periodic administrator tasks.
• Describe the basic functions of the Gaia operating system.
• Recognize SmartConsole features, functions, and tools.
• Understand how SmartConsole is used by administrators to give user access.
• Learn how Check Point security solutions and products work and how they protect networks.
• Understand licensing and contract requirements for Check Point security products.
• Describe the essential elements of a Security Policy.
• Understand the Check Point policy layer concept.
• Understand how to enable the Application Control and URL Filtering software.
• Blades to block access to various applications.
• Describe how to configure manual and automatic NAT.
• Identify tools designed to monitor data, determine threats and recognize opportunities for performance improvements.
• Describe different Check Point Threat Prevention solutions fornetwork attacks.
• Articulate how the Intrusion Prevention System is configured, maintained and tuned.
• Understand the Infinity Threat Prevention system.
• Knowledge about Check Point's IoT Protect.

**Check Point Certified Security Expert (CCSE)**

• Provide an overview of the upgrade service and options available.
• Explain how to perform management upgrade and migration.
• Articulate the process using CPUSE features.
• Articulate the purpose and function of Management High Availability.
• Explain Primary vs Secondary, Active vs Standby and Synchronization.
• Explain disaster recovery steps in case the primary management server becomes unavailable.
• Provide overview of Central Deployment in SmartConsole.
• Articulate an understanding of Security Gateway cluster upgrade methods.
• Explain about Multi Version Cluster (MVC) upgrades.
• Discuss Gaia Commands and how they are used.
• Explain the main processes on s and s.
• Describe how to work with scripts and SmartTasks to configure automatic actions.
• Explain the Management Data Plane Separation (MDPS).
• Explain kernel operations and traffic flow.
• Articulate Dynamic and Updatable Objects in Security Gateways.
• Explain the policy installation flow and files used.
• Describe the use of policy installation history.
• Explain concurrent and accelerated install policy.
• Describe an overview of APIs and ways to use and authenticate.
• Explain how to make changes in GAIA and management configuration.
• Explain how to install policy using API.
• Explain how the SecureXL acceleration technology enhances and optimizes Security Gateway performance.
• Describe how the CoreXL acceleration technology enhances and improves Security Gateway performance.
• Articulate how utilizing multiple traffic queues can make traffic handling more efficient.
• Discuss Site-to-Site VPN basics, deployment and communities.
• Describe how to analyze and interpret VPN tunnel traffic.
• Explain Link Selection and ISP Redundancy options.
• Explain tunnel management features.
• Discuss Check Point Remote Access solutions and how they differ from each other.
• Describe how client security can be provided by Remote Access .
• Explain authentication methods including machine authentication.
• Explain Multiple Entry Point (MEP).
• Discuss the Mobile Access Software Blade and how it secures communication and data exchange during remote connections.
• Describe Mobile Access deployment options.
• Discuss various features in Mobile Access like Portals, Link Translation, running Native Applications, Reverse Proxy and more.
• Explain basic concepts of Clustering and ClusterXL.
• Explain about Cluster Control Protocol (CCP) and synchronization.
• Describe advanced ClusterXL functions and modes like Load Sharing, Active-Active, VMAC mode etc.
• Discuss Cluster Correction Layer (CCL) to provide connection stickyness.
• Advanced Logs and Monitoring
• Explain how to determine if the configuration is compliant with the best practices.
• Explain how to set action items to meet the compliance.
• Discuss how SmartEvent functions to identify critical security issues.
• Describe the components of SmartEvent and their deployment options.
• Discuss how SmartEvent can assist in reporting security threats.
• Explain how to customize event definitions and set an Event Policy.

## Audience

Technical professionals who support, install deploy or administer Check Point products, and who perform advanced deployment configurations of Check Point products.

The Boot Camp courses helps delegates prepare for the CCSA and CCSE certification exams.

## Prerequisites

Working knowledge of Windows, UNIX, networking technology, the Internet and TCP/IP.

This course is not for new users to Check Point – previous certification/experience is required.

## Programme

**Check Point Certified Security Administrator (CCSA)**

• Configure the Security Management Server.
• Use the WebUI to run the First Time Wizard.
• Install the Smart Console.
• Install the Alpha Gateway using the network detailed in the course topology.
• Demonstrate how the Security Management Server and Gateway communicate.
• Test SIC Status.
• Create multiple administrators and apply different roles and permissions for simultaneous administration.
• Validate existing licenses for products installed on the network.
• Create and configure host, network and group objects.
• Create a simplified Security Policy.
• Demonstrate how to use Security Zones in policy.
• Demonstrate how to share a layer between Security Polices.
• Configure Network Address Translation for server and network objects.
• Enable Identity Awareness.
• Deploy user access roles for more granular control of the security Policy.
• Generate network Traffic and use traffic visibility tools to monitor the data.
• Use SmartConsole and SmartView Monitor to view status, alerts, and block suspicious traffic.

| | |
|---|---|
| **Check Point Certified Security Expert (CCSE)** | • Prepare for a Security Management Server Upgrade<br>• Upgrade the Security Management Server<br>• Deploy a Secondary Security Management Server<br>• Configure a Distributed Log Server<br>• Upgrade a Security Gateway from SmartConsole<br>• Work with the Command Line<br>• Use Scripts and SmartTasks<br>• Configure Dynamic Objects<br>• Monitor Traffic<br>• Verify Policy Installation and Status<br>• Work with Gaia and Management APIs<br>• Work with Acceleration Features<br>• Configure a Locally Managed Site to Site VPN<br>• Configure a Site to Site VPN with an Interoperable Device<br>• Configure Remote Access VPN<br>• Configure Mobile Access VPN<br>• Configure a High Availability Cluster<br>• Work with ClusterXL<br>• Configure Policy Compliance<br>• Deploy SmartEvent |

## Follow on courses

Attend two Infinity Specialization courses and pass their exams to automatically become a Check Point Certified Security Master (CCSM).

Attend four Infinity Specialization courses and pass their exams to automatically become a Check Point Certified Security Master Elite (CCSM Elite).

- Check Point Certified Endpoint Specialist (CCES)
- Check Point Certified Troubleshooting Administrator (CCTA)
- Check Point Certified Automation Specialist (CCAS)
- Check Point Certified Cloud Specialist (CCCS)
- Check Point Certified MDSM Specialist (CCMS)
- Check Point Certified VSX Specialist (CCVS)
- Check Point Certified Troubleshooting Expert (CCTE)
- Check Point Certified Maestro Expert (CCME)
- Check Point Certified Cloud Network Security Expert for AWS (CNSE-AWS)
- Check Point Certified Cloud Network Security Expert for Azure (CNSE-AZURE)

## Test and Certification

Prepare for exams #156-215.81 and #156-315.81 at www.VUE.com/checkpoint
Exam vouchers are available at an additional cost from educationteam.ecs.uk@arrow.com (0870 251 1000)
Full information on Check Point's Certification Program can be viewed at https://www.checkpoint.com/downloads/training/check-point-certification-faq.pdf

## Further Information

Please note that Check Point only offer e-kit courseware for training courses. Each delegate will be provided with an official set of e-kit courseware.

Arrow ECS are a Check Point Platinum Elite Authorised Training Company (ATC) Partner and participate in the Check Point Learning Credits (CLCs) and Partner Coop Training Program.

## Session Dates

On request. Please Contact Us

## Additional Information

This training is also available as onsite training. Please contact us to find out more.