Check Point Cybersecurity BootCamp R81.20
CCSA & CCSE

Certification to CCSA R81.20 and CCSE R81.20 normally requires attendance at two three-day courses. This BootCamp is ideal for participants who already have extensive experience with the Check Point Firewall and may have already completed a previous CCSA/CCSE certification.

In order to reach the certification goal faster, this five-day BootCamp covers all exam-relevant content and lab exercises of the two courses Check Point Certified Security Administrator R81.20 - CCSA and Check Point Certified Security Expert R81.20 - CCSE in a concentrated form. The extended course times (daily from 8 a.m. to 6 p.m.) form the time frame for the course. The lab is also available to participants around the clock during the course week for follow-up work and self-study of the content. At the end of the course, participants will have the knowledge to take the CCSA and CCSE R81.20 exams. Taking the exams is not part of this BootCamp.

Course Contents
CCSA - Security Administrator

- Security Management
- SmartConsole
- Deployment
- Object Management
- Licenses and Contracts
- Policy Rules and Rulebase
- Policy Packages
- Policy Layers
- Traffic Inspection
- Network Address Translation
- Application Control
- URL Filtering
- Logging
- Snapshots
- Backup and Restore
- Gaia
- Permissions
- Policy Installation

CCSE - Security Expert

- Advanced Deployments
- Management High Availability
- Advanced Gateway Deployment
- Advanced Policy Configuration
- Advanced User Access Management
- Custom Threat Protection
- Advanced Site-to-Site VPN
- Remote Access VPN
- Mobile Access VPN
- Advanced Security Monitoring
- Performance Tuning
- Advanced Security Maintenance

E-Book You will receive the original documentation as a Check Point e-Kit.

Target Group
This course is aimed at participants who have experience in working with Check Point Firewalls and would like to learn the knowledge from the CCSA R81.20 and CCSE R81.20 courses in a compact form

Prerequisites
One year of experience with Check Point products. Working knowledge of Windows, UNIX, network technology, Internet and TCP/IP is recommended.

Course Target
CCSA - Security Administrator

- Describe the major components of a three-tier Check Point architecture and explain how they work together in the Check Point environment.
- Identify the basic workflow for installing the Security Management Server and Security Gateway for a single-domain solution.
- Create SmartConsole objects that match the organization's topology for use in policies and rules.
- Identify the tools available to manage Check Point licenses and contracts, including their purpose and use.
- Identify features and functionality that enhance security policy configuration and management.
- Demonstrate your understanding of Application Control & URL Filtering and Autonomous Threat Prevention and how to configure these solutions to meet an organization's security needs.
- Describe how to analyze and interpret VPN tunnel traffic.
- Describe how to monitor the health of supported Check Point hardware using Gaia Portal and the command line.
- Describe the various methods for securing Check Point system information and discuss best practices and recommendations for each method.

CCSE - Security Expert

- Identify the types of technologies Check Point supports for automation
- Explain the purpose of the Check Management High Availability (HA) deployment
- Explain the basic concepts of clustering and ClusterXL, including protocols, synchronization, and connection stability.
- Explain the purpose of dynamic objects, updatable objects, and network feeds.
- Describe the components and configurations of Identity Awareness.
- Describe the different Check Point Threat Prevention solutions.
- Explain how to configure the Intrusion Prevention System.
- Explain the purpose of domain-based VPNs.
- Describe situations where externally managed certificate authentication is used.
- Describe how client security can be ensured through remote access.
- Explain the Mobile Access Software Blade.
- Define performance optimization solutions and basic configuration procedures.
- Identify supported upgrade methods and procedures for security gateways.

Status 06/19/2025

This Course in the Web
You can find the up-to-date information and options for ordering under the following link: www.experteach-training.com/go/**CPB8**

Reservation
On our Website, you can reserve a course seat for 7 days free of charge and in an non-committal manner. This can also be done by phone under +49 6074/4868-0.

Guaranteed Course Dates
To ensure reliable planning, we are continuously offering a wide range of guaranteed course dates.

Your Tailor-Made Course!
We can precisely customize this course to your project and the corresponding requirements.

Training		Prices, excl. of V.A.T.
Classes in Germany	**5 Days**	**€ 3,595**
Online Training	**5 Days**	**€ 3,595**
Date/course venue	Course language German	
10/11-14/11/25 Frankfurt	13/04-17/04/26 Frankfurt	
10/11-14/11/25 Online	13/04-17/04/26 Online	

Our Training Offer for You:

Classroom Training
The live training experience in our training centers or on your premises on-site.

Online Training
Attend your course in online mode – without travel and accommodation expenses and effort.

Hybrid Training
Classroom & online in one course – choose how you wish to participate in your training event.

In-house Training
We create your customized training concepts for your project.

Guaranteed Course Dates
ExperTeach guaranteed course dates allow for secure and reliable planning.

Awards Won by ExperTeach