



CHECK POINT HARMONY ENDPOINT SPECIALIST (CCES)



AUDIENCE

This course is designed for Security Administrators who are responsible for deploying and managing a Harmony Endpoint security solution.



GOALS

Demonstrate an understanding of the Check Point Harmony Endpoint solution, including its features and capabilities. Apply knowledge and skills gained during training to manage and protect a Harmony Endpoint solution.



PREREQUISITES

Working knowledge of Unix-like and/or Windows operating systems, networking fundamentals, networking security, TCP/IP networking, administration.

TOPICS

Introduction to Harmony Endpoint

Harmony Endpoint Security Management

Deploying Harmony Endpoint

Data Security Protection

Advanced Threat Prevention

Large-Scale Harmony Endpoint Deployment

Troubleshooting

Harmony Endpoint Management as a Service

OBJECTIVES

- Describe Check Point Infinity's Consolidated Security Architecture.
- Explain the difference between the Harmony Endpoint On-Premises and Cloud management environments.
- Identify the main components of the Harmony Endpoint Security Architecture.
- Identify the basic workflow for Harmony Endpoint Security Management.
- Give examples of useful resources for Harmony Endpoint Security Management.
- Log in to the Web Management Console.
- Navigate the Web Management interface to gain a basic understanding of the features and capabilities Harmony Endpoint provides for security management.
- Discuss situations where it might be necessary to change default policy rules.
- Identify recommended releases for a Harmony Endpoint Client deployment.
- Identify deployment prerequisites.
- Given a deployment scenario, identify deployment methods, Endpoint Client packages, and the basic workflow.
- Recognize the different types of data security available to deploy.
- Describe how Full Disk Encryption protects and recovers data that is accessed and stored on Endpoint computers.
- Identify how to secure removable media devices and protect ports.
- Identify remote help and recovery capabilities.
- Discuss the challenges of threat prevention.
- Identify how Harmony Endpoint defends networks against advanced threats.
- Identify the key components in Harmony Endpoint simplified and large-scale deployments.
- Identify sizing guidelines for Harmony Endpoint deployments.
- Give examples of how to expand the solution with Super Nodes and External Policy Servers.
- Identify the additional capabilities that High Availability (HA) and Active Directory configurations support.
- Identify useful resources for basic troubleshooting.
- Give examples of potential problems or issues that might occur when using Harmony Endpoint.
- Investigate and troubleshoot basic Harmony Endpoint troubleshooting scenarios.
- Define Harmony Endpoint Management as a Service.
- Explain the set-up process for Harmony Endpoint Management as a Service.
- Discuss the workflow when migrating from Endpoint On-Premises to Endpoint Management as a Service.

EXERCISES

- Install the Endpoint Security Management Server
- Deploy an Endpoint Security Management Server
- Configure Endpoint for Deployment
- Deploy Endpoint Security Clients to Hosts
- Test and Analyze Threat Response
- Configure LDAP Strong Authentication
- Deploy a Secondary Endpoint Security Management Server
- Troubleshoot Endpoint Communication Issues
- Migrate from On-Premises to Endpoint Management as a Service (Optional)
- Connect Existing Hosts to Endpoint Management as a Service (Optional)

CERTIFICATION INFORMATION

CCES

Prepare for exam #156-536 [VUE.com/checkpoint](https://www.checkpoint.com)

© 2023 Check Point Software Technologies Ltd. All rights reserved.
[Protected] Non-confidential content – DOC-TDS-CCES-R81.20-V1.0