KL 002.11: Kaspersky Endpoint Security and Management. Fundamentals

Title	Kaspersky Endpoint Security and Management. Fundamentals
Code	KL 002.11
Target group	Microsoft Windows network administrators, information security specialists, technical support engineers, presales engineers
Featured products	Kaspersky Security Center 10 SP3 Kaspersky Endpoint Security 11
Recommended for preparation for the following exams	KLE 002.11: Kaspersky Endpoint Security and Management. Fundamentals
Duration	3 days

The course prepares for planning, deployment and maintenance of Windows network protection systems based on Kaspersky Endpoint Security and managed via Kaspersky Security Center. It tells about those solutions that can help to protect a network of approximately up to 1000 endpoints in a single location. Endpoints in this course are servers and workstations running Windows.

The lectures and laboratory sessions provide the audience with the necessary knowledge and skill to be able to:

- Describe the capabilities of Kaspersky Endpoint Security for Windows and Kaspersky Security Center
- Plan and implement an optimal Windows network protection solution based on Kaspersky Endpoint Security and managed via Kaspersky Security Center
- Administer the deployed system

Course Syllabus

Unit I. Deployment

Chapter 1. How to deploy Kaspersky Endpoint Security for Business
Chapter 2. How to deploy Kaspersky Security Center
- Lab 1.1 — Installing Kaspersky Security Center

Chapter 3. How to deploy Kaspersky Endpoint Security on computers
- Lab 1.2 — Deploying Kaspersky Endpoint Security
- Lab 1.3 — Installing Kaspersky Endpoint Security for Windows on Mobile Computer

Chapter 4. How to arrange computers into groups
- Lab 1.4 — Creating Managed Computers Structure

Unit II. Protection Management

Chapter 1. How Kaspersky Endpoint Security protects a computer

Chapter 2. Configuring file system protection
- Lab 2.1 — Configuring File Anti-Virus
- Lab 2.2 — Configuring virus scan tasks
- Lab 2.3 — Configuring exceptions for folders

Chapter 3. Configuring network protection
- Lab 2.4 — Configuring exceptions for Web Anti-Virus
- Lab 2.5 — Configuring Mail Anti-Virus
- Lab 2.6 — Configuring Network Attack Blocker

Chapter 4. How to protect against advanced threats
- Lab 2.7 — Configuring protection against ransomware

Chapter 5. Controlling network connections
Chapter 6. Protecting out-of-office computers
- Lab 2.8 — Configuring Firewall for out-of-office computers

Chapter 7. Other protection settings
- Lab 2.9 — Configuring exceptions from Self-Defense
- Lab 2.10 — Configuring password protection for Kaspersky Endpoint Security

Unit III. Control
Chapter 1. Introduction
Chapter 2. Application Control
- Lab 3.1 — Configuring application startup control
- Lab 3.2 — Blocking the startup of programs on the network

Chapter 3. Device Control

- Lab 3.3 — Denying access to USB Flash Drives
- Lab 3.4 — Setting permissions for removable drives

Chapter 4. Web Control
- Lab 3.5 — Configuring Web Control

Unit IV. Maintenance

Chapter 1. How to maintain the protection
Chapter 2. Daily tasks
- Lab 4.1 — Configuring dashboards
- Lab 4.2 — Configuring helper tool

Chapter 3. Handling incidents
- Lab 4.3 — Collecting traces

Chapter 4. Rare and irregular activitie
- Lab 4.4 — Backup and Restore in Kaspersky Security Center

Requirements for the Students

To be able to master the course and efficiently fulfill the laboratory work, the students must possess the following knowledge and skills:
- Understanding of TCP/IP, the Internet and e-mail operating principles, basic skills in administering Microsoft Windows networks and Active Directory
- Experience with Microsoft Windows operating systems
  All participants receive an official certificate after course completion.