

DOCUMENT* PRESENTED
BY WICK HILL

access
access
management
management
performance
performance
security
security
Convergence
Convergence

Wick Hill plc, River Court, Albert Drive, Woking, Surrey, GU21 5RP
01483 227600 | www.wickhill.com | info@wickhill.com

* © Wick Hill and the Wick Hill logo are trademarks of Wick Hill Group Plc. Registered in the UK and other countries. Other logo, brand and product names are trademarks of their respective owners. All 3rd party information contained within this document is copyright of the originator. Errors and omissions excluded.



Kaspersky®

Endpoint Security for Windows

Contents

Unit I. Deployment

Chapter 1. Organizational Issues

Chapter 2. Installation of Kaspersky Security Center

Chapter 3. Installation on Computers

Chapter 4. Management of Computer Structure

- Practice 1.1 — Installing Kaspersky Security Center
- Practice 1.2 — Deploying KES
- Practice 1.3 — Installing KES on Mobile Computer
- Practice 1.4 — Creating Managed Computers Structure
- Practice 1.5 — Monitoring protection deployment

Unit II. Protection Management

Chapter 1. Basics of Kaspersky Endpoint Security 8.0

Chapter 2. File System Protection

Chapter 3. Network Protection

Chapter 4. Proactive Defense

Chapter 5. Threat Diagnostics

Chapter 6. Protection Status Diagnostics

- Practice 2.1 — Tasks and Policies Creation
- Practice 2.2 — Checking File Anti-Virus
- Practice 2.3 — Identification of unreliable users
- Practice 2.4 — Configuring Firewall
- Practice 2.5 — Processing virus incidents
- Practice 2.6 — Configuring Exceptions

Unit III. Control

Chapter 1. Application Control

Chapter 2. Fixing Vulnerabilities

Chapter 3. Device Control

Chapter 4. Web Control

- Practice 3.1 — Browser Start Control
- Practice 3.2 — Application Startup Control
- Practice 3.3 — Blocking USB Flash Drives
- Practice 3.4 — Access Rights for USB Flash Drives
- Practice 3.5 — Web Access Control

Unit IV. Maintenance

Chapter 1. Statistics and Reports

Chapter 2. Updates

Chapter 3. License Management

Chapter 4. Interaction with User

Chapter 5. Mobile Computer Management

Chapter 6. Backup and Restore

- Practice 4.1 — Database Update and License Renewal
- Practice 4.2 — Password Protection for KES
- Practice 4.3 — Hiding KES
- Practice 4.4 — Configuring Mobile Computer Protection
- Practice 4.5 — Backup and Restore