kaspersky

Kaspersky Security Center

(version 13.0.0.11247)

Security Target

Document version: 2.02

08.11.2021

Document history

Date	Version	Author	Change
March 2019	1.01	Oleg Andrianov	Document creation – first version
June 2019	1.02	Oleg Andrianov	Corrections following ORs.
July 2019	1.03	Oleg Andrianov	Corrections following ORs.
December 2019	1.04	Alexander Testov	Corrections following ORs.
March 2021	2.00	Alexander Testov	First draft for KSC 13.
September 2021	2.01	Alexander Testov	Corrections due to observation reports.
November 2021	2.02	Alexander Testov	Corrections due to observation reports.

Table of Contents

Terminology

This Security Target refers to the terms, definitions and abbreviations of Sections 4 and 5 of [CCp1].

Additionally, the following terms and abbreviations, most of which specific to Kaspersky products, shall be defined.

Term	Definition
AV	Anti-Virus Software
AES	Advanced Encryption Standard
ECDHE	Elliptic-Curve Diffie–Hellman Ephemeral
KES	Kaspersky Endpoint Security
KSC	Kaspersky Security Center
LAN	Local Area Network
RDBMS	Relational database management system
RSA	Rivest, Shamir and Adleman algorithm
SHA	Secure Hash Algorithm
TLS	Transport Layer Security
Malware	Malicious software that is specifically designed to disrupt, damage, or gain unauthorised access to a computer system and disrupt of information confidentiality, integrity and availability.
Virus	While technically computer virus is just a type of malware—specifically replicating file infector—this term, however, is often used to describe malware in general. In this document ‘virus’ means ‘malware’.

1 ST Introduction

1.1 ST Reference

Title	Kaspersky Security Center. Security Target
Sponsor	AO Kaspersky Lab
Author(s)	Oleg Andrianov, AO Kaspersky Lab Alexander Testov, AO Kaspersky Lab
ST Version	2.02
ST Publication Date	8 November 2021
CC Version	Version 3.1, Revision 5
Assurance Level	EAL2+ (EAL2 augmented with ALC_FLR.1)

1.2 TOE Reference

1 The target of evaluation (TOE) in this ST is **Kaspersky Security Center (version 13.0.0.11247)** developed by AO Kaspersky Lab.

1.3 TOE Overview

1.3.1 TOE type

2 The TOE is Kaspersky Security Center (also referred to as KSC), a software application designed for centralised management of other Kaspersky Lab security (primarily anti-virus) software applications installed on separate endpoint devices (for example, Kaspersky Endpoint Security for Windows), and, to some extent, for centralised management of those endpoint devices themselves.

1.3.2 TOE usage and major security features

3 The TOE implements the following three security functionalities.

4 **Audit**. The TOE generates audit records for its own audible events, and collects audit records from Kaspersky Lab security software installed on the managed endpoint devices, and provides means for audit reviewing.

5 **Administration**. The TOE is able to remotely collect data from Kaspersky Lab security software installed on endpoint devices in an organization's LAN, and manage this software. Providing these administration capabilities, the TOE ensures that only authorised users are able to access this functionality. The TOE provides identification/authentication and role-based access control for the TOE administration.

6 **Protected communications.** The implemented security mechanisms are oriented to protect the communications between physically divided parts of the TOE, ensuring the security of the sensitive data being sent from/to the managed devices. The communication used for the remote administration of the TOE is also protected by establishing a trusted channel to Web Console, which is not a part of the TOE.

1.3.3 Required Non-TOE software and hardware

7 For correct functioning the TOE requires certain hardware and software. Below requirements are listed as described on Figure 1:

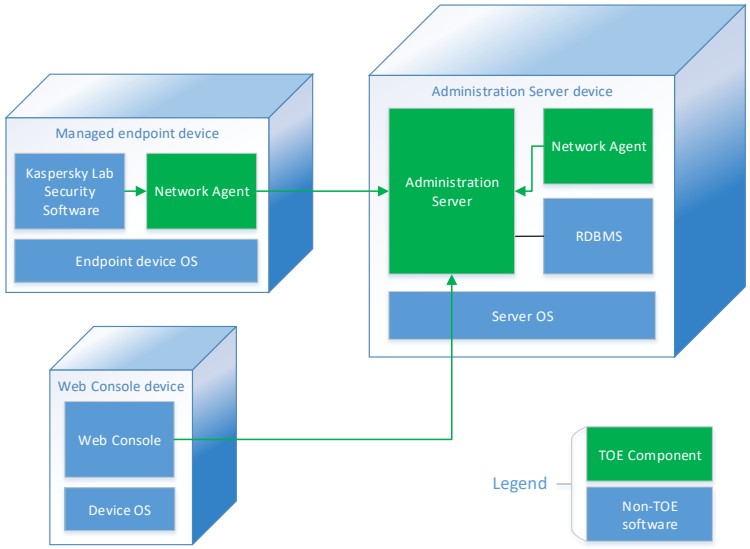

Figure 1. General physical overview

1.3.3.1 Administration Server

1.3.3.1.1 Minimum hardware requirements:

- CPU with operating frequency of 1 GHz or higher. For a 64-bit operating system, the minimum CPU frequency is 1.4 GHz.
- RAM: 4 GB.
- Available disk space: 10 GB. When Vulnerability and Patch Management is used, at least 100 GB of free disk space must be available.

For deployment in cloud environments, the requirements for Administration Server and database server are the same as the requirements for physical Administration Server.

1.3.3.1.2 Software requirements:

- Microsoft Data Access Components (MDAC) 2.8
- Microsoft Windows DAC 6.0
- Microsoft Windows Installer 4.5
- Operating system, one of the following:
  - Microsoft Windows 10 20H2 32-bit/64-bit (all editions)
  - Microsoft Windows 10 20H1 32-bit/64-bit (all editions)
  - Microsoft Windows 10 Enterprise 2019 LTSC 32-bit/64-bit
  - Microsoft Windows 10 Enterprise 2016 LTSB 32-bit/64-bit
  - Microsoft Windows 10 Enterprise 2015 LTSB 32-bit/64-bit
  - Microsoft Windows 10 Pro RS5 (October 2018 Update, 1809) 32-bit/64-bit
  - Microsoft Windows 10 Pro for Workstations RS5 (October 2018 Update, 1809) 32-bit/64-bit
  - Microsoft Windows 10 Enterprise RS5 (October 2018 Update, 1809) 32-bit/64-bit
  - Microsoft Windows 10 Education RS5 (October 2018 Update, 1809) 32-bit/64-bit
  - Microsoft Windows 10 Pro 19H1 32-bit/64-bit
  - Microsoft Windows 10 Pro for Workstations 19H1 32-bit/64-bit
  - Microsoft Windows 10 Enterprise 19H1 32-bit/64-bit

  - Microsoft Windows 10 Education 19H1 32-bit/64-bit
  - Microsoft Windows 10 Home 19H2 32-bit/64-bit
  - Microsoft Windows 10 Pro 19H2 32-bit/64-bit
  - Microsoft Windows 10 Pro for Workstations 19H2 32-bit/64-bit
  - Microsoft Windows 10 Enterprise 19H2 32-bit/64-bit
  - Microsoft Windows 10 Education 19H2 32-bit/64-bit
  - Microsoft Windows 8.1 Pro 32-bit/64-bit
  - Microsoft Windows 8.1 Enterprise 32-bit/64-bit
  - Microsoft Windows 8 Pro 32-bit/64-bit
  - Microsoft Windows 8 Enterprise 32-bit/64-bit
  - Microsoft Windows 7 Professional with Service Pack 1 and higher 32-bit/64-bit
  - Microsoft Windows 7 Enterprise/Ultimate with Service Pack 1 and higher 32-bit/64-bit
  - Windows Server 2019 Standard 64-bit
  - Windows Server 2019 Core 64-bit
  - Windows Server 2019 Datacenter 64-bit
  - Windows Server 2016 Server Standard RS3 (v1709) (LTSB/CBB) 64-bit
  - Windows Server 2016 Server Datacenter RS3 (v1709) (LTSB/CBB) 64-bit
  - Windows Server 2016 Server Core RS3 (v1709) (Installation Option) (LTSB/CBB) 64-bit
  - Windows Server 2016 Standard (LTSB) 64-bit
  - Windows Server 2016 Server Core (Installation Option) (LTSB) 64-bit
  - Windows Server 2016 Datacenter (LTSB) 64-bit
  - Windows Server 2012 R2 Standard 64-bit
  - Windows Server 2012 R2 Server Core 64-bit
  - Windows Server 2012 R2 Foundation 64-bit
  - Windows Server 2012 R2 Essentials 64-bit
  - Windows Server 2012 R2 Datacenter 64-bit
  - Windows Server 2012 Standard 64-bit
  - Windows Server 2012 Server Core 64-bit
  - Windows Server 2012 Foundation 64-bit
  - Windows Server 2012 Essentials 64-bit
  - Windows Server 2012 Datacenter 64-bit
  - Windows Server 2008 R2 Standard with Service Pack 1 and higher 64-bit
  - Windows Server 2008 R2 with Service Pack 1 (all editions) 64-bit
  - Windows Storage Server 2016 64-bit
  - Windows Storage Server 2012 R2 64-bit
  - Windows Storage Server 2012 64-bit
- Database server (can be installed on a different device), one of the folllowing:
  - Microsoft SQL Server 2012 Express 64-bit
  - Microsoft SQL Server 2014 Express 64-bit
  - Microsoft SQL Server 2016 Express 64-bit
  - Microsoft SQL Server 2017 Express 64-bit
  - Microsoft SQL Server 2019 Express 64-bit
  - Microsoft SQL Server 2014 (all editions) 64-bit
  - Microsoft SQL Server 2016 (all editions) 64-bit
  - Microsoft SQL Server 2017 (all editions) on Windows 64-bit
  - Microsoft SQL Server 2017 (all editions) on Linux 64-bit
  - Microsoft SQL Server 2019 (all editions) on Windows 64-bit (requires additional actions[1])
  - Microsoft SQL Server 2019 (all editions) on Linux 64-bit (requires additional actions[2])
  - MySQL Standard Edition 5.7 32-bit/64-bit
  - MySQL Enterprise Edition 5.7 32-bit/64-bit
  - All supported SQL Server editions in Amazon RDS and Microsoft Azure cloud platforms
  - MariaDB Server 10.3 32-bit/64-bit with InnoDB storage engine[3]

[1] https://help.kaspersky.com/KSC/13/en-US/92403.htm
[2] https://help.kaspersky.com/KSC/13/en-US/92403.htm
[3] It is recommended to use MariaDB 10.3.22; if use an earlier version, the Perform Windows update task might take more than one day to work.

- The following virtualization platforms are supported:
  - VMware vSphere 6.7
  - VMware vSphere 7.1
  - VMware Workstation 15 Pro
  - VMware Workstation 16 Pro
  - Microsoft Hyper-V Server 2012 64-bit
  - Microsoft Hyper-V Server 2012 R2 64-bit
  - Microsoft Hyper-V Server 2016 64-bit
  - Microsoft Hyper-V Server 2019 64-bit
  - Citrix XenServer 7.1 LTSR
  - Citrix XenServer 8.x
  - Parallels Desktop 16
  - Oracle VM VirtualBox 6.x (Windows guest login only)
- The following SIEM systems are supported:
  - HP (Micro focus) ArcSight ESM 7.0
  - HP (Micro focus) ArcSight ESM 6.8
  - IBM QRadar 7.4

1.3.3.2 Web Console

8 Kaspersky Security Center 13 Web Console (also referred to as Web Console) is an application that uses a web interface (Open API) provided by KSC for its management. Web Console is not a part of the TOE.

1.3.3.2.1 Web Console Server minimum hardware requirements:

- CPU: 4 cores, operating frequency of 2.5 GHz
- RAM: 8 GB
- Available disk space: 40 GB

1.3.3.2.2 Web Console Server Software requirements:

- Operating system Microsoft Windows (64-bit versions only), one of the following:
  - Microsoft Windows 10 20H2 (all editions)
  - Microsoft Windows 10 20H1 (all editions)
  - Microsoft Windows 10 Enterprise 2019 LTSC
  - Microsoft Windows 10 Enterprise 2016 LTSB
  - Microsoft Windows 10 Enterprise 2015 LTSB
  - Microsoft Windows 10 Pro RS5 (October 2018 Update, 1809)
  - Microsoft Windows 10 Pro for Workstations RS5 (October 2018 Update, 1809)
  - Microsoft Windows 10 Enterprise RS5 (October 2018 Update, 1809)
  - Microsoft Windows 10 Education RS5 (October 2018 Update, 1809)
  - Microsoft Windows 10 Pro 19H1
  - Microsoft Windows 10 Pro for Workstations 19H1
  - Microsoft Windows 10 Enterprise 19H1
  - Microsoft Windows 10 Education 19H1
  - Microsoft Windows 10 Home 19H2
  - Microsoft Windows 10 Pro 19H2
  - Microsoft Windows 10 Pro for Workstations 19H2
  - Microsoft Windows 10 Enterprise 19H2
  - Microsoft Windows 10 Education 19H2
  - Microsoft Windows 8.1 Pro
  - Microsoft Windows 8.1 Enterprise
  - Windows Server 2019 Standard
  - Windows Server 2019 Core
  - Windows Server 2019 Datacenter
  - Windows Server 2016 Server Standard RS3 (v1709) (LTSB/CBB)
  - Windows Server 2016 Server Datacenter RS3 (v1709) (LTSB/CBB)
  - Windows Server 2016 Server Core RS3 (v1709) (Installation Option) (LTSB/CBB)

  - Windows Server 2016 Standard (LTSB)
  - Windows Server 2016 Server Core (Installation Option) (LTSB)
  - Windows Server 2016 Datacenter (LTSB)
  - Windows Server 2012 R2 Standard
  - Windows Server 2012 R2 Server Core
  - Windows Server 2012 R2 Foundation
  - Windows Server 2012 R2 Essentials
  - Windows Server 2012 R2 Datacenter
  - Windows Server 2012 Standard
  - Windows Server 2012 Server Core
  - Windows Server 2012 Foundation
  - Windows Server 2012 Essentials
  - Windows Server 2012 Datacenter
  - Windows Storage Server 2016
  - Windows Storage Server 2012 R2
  - Windows Storage Server 2012
- Linux (64-bit versions only):
  - Debian GNU/Linux 10.x (Buster)
  - Debian GNU/Linux 9.x (Stretch)
  - Ubuntu Server 20.04 LTS (Focal Fossa)
  - Ubuntu Server 18.04 LTS (Bionic Beaver)
  - CentOS 8.x
  - CentOS 7.x
  - Red Hat Enterprise Linux Server 8.x
  - Red Hat Enterprise Linux Server 7.x
  - SUSE Linux Enterprise Server 15 (all Service Packs)
  - SUSE Linux Enterprise Server 12 (all Service Packs)
  - Astra Linux Special, version 1.6
  - Astra Linux Special, version 1.5
  - Astra Linux Common Edition, version 2.12
  - ALT 9.1
  - ALT 8.3
  - ALT SE 8

1.3.3.2.3 Client devices hardware and software requirements

9 For a client device, use of Kaspersky Security Center 13 Web Console requires only a browser.

10 The hardware and software requirements for the device are identical to the requirements of the browser that is used with Kaspersky Security Center 13 Web Console.

- Browser:
  - Mozilla Firefox 68 Extended Support Release
  - Mozilla Firefox 68 or later
  - Google Chrome 75 or later
  - Safari 12 on macOS
  - Safari 13 on iOS

1.3.3.3 Administration Console

1.3.3.3.1 Hardware requirements:

- CPU: with operating frequency of 1 GHz or higher. For a 64-bit OS, the minimum CPU frequency is 1.4 GHz.
- RAM: 512 MB.
- Available disk space: 1 GB.

1.3.3.3.2 Software requirements:

- Microsoft Windows operating system (supported version of the operating system is determined by the requirements of Administration Server), **except** for the following operating systems:
  - Windows Server 2012 Server Core 64-bit
  - Windows Server 2012 R2 Server Core 64-bit
  - Windows Server 2016 Server Core (Installation Option) (LTSB) 64-bit
  - Windows Server 2016 Server Datacenter RS3 (v1709) (LTSB/CBB) 64-bit
  - Windows Server 2016 Server Standard RS3 (v1709) (LTSB/CBB) 64-bit
  - Windows Server 2016 Server Core RS3 (v1709) (Installation Option) (LTSB/CBB) 64-bit
  - Windows Server 2019 Core 64-bit
- Microsoft Management Console 2.0
- Microsoft Windows Installer 4.5
- Microsoft Internet Explorer 10.0 running on:
  - Microsoft Windows Server 2008 R2 Service Pack 1
  - Microsoft Windows Server 2012
  - Microsoft Windows Server 2012 R2
  - Microsoft Windows 7 Service Pack 1
  - Microsoft Windows 8
  - Microsoft Windows 8.1
  - Microsoft Windows 10
- Microsoft Internet Explorer 11.0 running on:
  - Microsoft Windows Server 2012 R2
  - Microsoft Windows Server 2012 R2 Service Pack 1
  - Microsoft Windows Server 2016
  - Microsoft Windows Server 2019
  - Microsoft Windows 7 Service Pack 1
  - Microsoft Windows 8.1
  - Microsoft Windows 10
- Microsoft Edge running on Microsoft Windows 10

1.3.3.4 Network Agent (on a managed endpoint device)

1.3.3.4.1 Minimum hardware requirements:

- CPU with operating frequency of 1 GHz or higher. For a 64-bit OS, the minimum CPU frequency is 1.4 GHz.
- RAM: 512 MB.
- Available disk space: 1 GB.

1.3.3.4.2 Software requirements:

- Operating system, one of the following:
  - Microsoft Windows Embedded POSReady 2009 with latest Service Pack 32-bit
  - Microsoft Windows Embedded POSReady 7 32-bit/64-bit
  - Microsoft Windows Embedded Standard 7 with Service Pack 1 32-bit/64-bit
  - Microsoft Windows Embedded 8 Standard 32-bit/64-bit
  - Microsoft Windows Embedded 8.1 Industry Pro 32-bit/64-bit
  - Microsoft Windows Embedded 8.1 Industry Enterprise 32-bit/64-bit
  - Microsoft Windows Embedded 8.1 Industry Update 32-bit/64-bit
  - Microsoft Windows 10 20H2 32-bit/64-bit (all editions)
  - Microsoft Windows 10 20H1 32-bit/64-bit (all editions)
  - Microsoft Windows 10 Enterprise 2015 LTSB 32-bit/64-bit
  - Microsoft Windows 10 Enterprise 2016 LTSB 32-bit/64-bit
  - Microsoft Windows 10 Enterprise 2019 LTSC 32-bit/64-bit
  - Microsoft Windows 10 Home RS5 (Oct 2018) 32-bit/64-bit
  - Microsoft Windows 10 Pro RS5 (Oct 2018) 32-bit/64-bit
  - Microsoft Windows 10 Pro for Workstations RS5 (Oct 2018) 32-bit/64-bit
  - Microsoft Windows 10 Enterprise RS5 (Oct 2018) 32-bit/64-bit

- Microsoft Windows 10 Education RS5 (Oct 2018) 32-bit/64-bit
- Microsoft Windows 10 Home RS4 (April 2018 Update, 17134) 32-bit/64-bit
- Microsoft Windows 10 Pro RS4 (April 2018 Update, 17134) 32-bit/64-bit
- Microsoft Windows 10 Pro for Workstations RS4 (April 2018 Update, 17134) 32-bit/64-bit
- Microsoft Windows 10 Enterprise RS4 (April 2018 Update, 17134) 32-bit/64-bit
- Microsoft Windows 10 Education RS4 (April 2018 Update, 17134) 32-bit/64-bit
- Microsoft Windows 10 Home RS3 (Fall Creators Update, v1709) 32-bit/64-bit
- Microsoft Windows 10 Pro RS3 (Fall Creators Update, v1709) 32-bit/64-bit
- Microsoft Windows 10 Pro for Workstations RS3 (Fall Creators Update, v1709) 32-bit/64-bit
- Microsoft Windows 10 Enterprise RS3 (Fall Creators Update, v1709) 32-bit/64-bit
- Microsoft Windows 10 Education RS3 (Fall Creators Update, v1709) 32-bit/64-bit
- Microsoft Windows 10 Home 19H1 32-bit/64-bit
- Microsoft Windows 10 Pro 19H1 32-bit/64-bit
- Microsoft Windows 10 Pro for Workstations 19H1 32-bit/64-bit
- Microsoft Windows 10 Enterprise 19H1 32-bit/64-bit
- Microsoft Windows 10 Education 19H1 32-bit/64-bit
- Microsoft Windows 10 Home 19H2 32-bit/64-bit
- Microsoft Windows 10 Pro 19H2 32-bit/64-bit
- Microsoft Windows 10 Pro for Workstations 19H2 32-bit/64-bit
- Microsoft Windows 10 Enterprise 19H2 32-bit/64-bit
- Microsoft Windows 10 Education 19H2 32-bit/64-bit
- Microsoft Windows 8.1 Pro 32-bit/64-bit
- Microsoft Windows 8.1 Enterprise 32-bit/64-bit
- Microsoft Windows 8 Pro 32-bit/64-bit
- Microsoft Windows 8 Enterprise 32-bit/64-bit
- Microsoft Windows 7 Professional with Service Pack 1 and higher 32-bit/64-bit
- Microsoft Windows 7 Enterprise/Ultimate with Service Pack 1 and higher 32-bit/64-bit
- Microsoft Windows 7 Home Basic/Premium with Service Pack 1 and higher 32-bit/64-bit
- Microsoft Windows XP Professional for Embedded Systems 32-bit
- Microsoft Windows XP Professional Service Pack 3 and higher 32-bit
- Windows Small Business Server 2011 Essentials 64-bit
- Windows Small Business Server 2011 Premium Add-on 64-bit
- Windows Small Business Server 2011 Standard 64-bit
- Windows MultiPoint Server 2011 Standard/Premium 64-bit
- Windows MultiPoint Server 2012 Standard/Premium 64-bit
- Windows Server 2008 R2 Standard Service Pack 1 and higher 64-bit
- Windows Server 2008 R2 Datacenter Service Pack 1 and higher 64-bit
- Windows Server 2008 R2 Enterprise Service Pack 1 and higher 64-bit
- Windows Server 2008 R2 Foundation with Service Pack 1 and higher 64-bit
- Windows Server 2008 R2 Service Pack 1 and higher Core Mode 64-bit
- Windows Server 2008 R2 Service Pack 1 (all editions) 64-bit
- Windows Server 2012 Server Core 64-bit
- Windows Server 2012 Datacenter 64-bit
- Windows Server 2012 Essentials 64-bit
- Windows Server 2012 Foundation 64-bit
- Windows Server 2012 Standard 64-bit
- Windows Server 2012 R2 Server Core 64-bit
- Windows Server 2012 R2 Datacenter 64-bit
- Windows Server 2012 R2 Essentials 64-bit
- Windows Server 2012 R2 Foundation 64-bit
- Windows Server 2012 R2 Standard 64-bit
- Windows Server 2016 Datacenter (LTSB) 64-bit
- Windows Server 2016 Standard (LTSB) 64-bit
- Windows Server 2016 Server Core (Installation Option) (LTSB) 64-bit
- Windows Server 2016 Server Datacenter RS3 (v1709) (LTSB/CBB) 64-bit
- Windows Server 2016 Server Standard RS3 (v1709) (LTSB/CBB) 64-bit

  - Windows Server 2016 Server Core RS3 (v1709) (Installation Option) (LTSB/CBB) 64-bit
  - Windows Server 2019 Standard 64-bit
  - Windows Server 2019 Core 64-bit
  - Windows Server 2019 Datacenter 64-bit
  - Windows Storage Server 2016 64-bit
  - Windows Storage Server 2012 64-bit
  - Windows Storage Server 2012 R2 64-bit
  - Debian GNU/Linux 10.x (Buster) 32-bit/64-bit
  - Debian GNU/Linux 9.x (Stretch) 32-bit/64-bit
  - Ubuntu Server 20.04 LTS (Focal Fossa) 32-bit/64-bit
  - Ubuntu Server 18.04 LTS (Bionic Beaver) 32-bit/64-bit
  - Ubuntu Desktop 20.04 LTS (Focal Fossa) 32-bit/64-bit
  - Ubuntu Desktop 18.04 LTS (Bionic Beaver) 32-bit/64-bit
  - CentOS 8.x 64-bit
  - CentOS 7.x 64-bit
  - Red Hat Enterprise Linux Server 8.x 64-bit
  - Red Hat Enterprise Linux Server 7.x 64-bit
  - SUSE Linux Enterprise Server 15 (all Service Packs) 64-bit
  - SUSE Linux Enterprise Desktop 15 (all Service Packs) 64-bit
  - SUSE Linux Enterprise Server 12 (all Service Packs) 64-bit
  - Astra Linux Special, version 1.6
  - Astra Linux Special, version 1.5
  - Astra Linux Common Edition, version 2.12
  - ALT 9.1
  - ALT 8.3
  - ALT SE 8
  - OS X 10.10 (Yosemite)
  - OS X 10.11 (El Capitan)
  - macOS Sierra (10.12)
  - macOS High Sierra (10.13)
  - macOS Mojave (10.14)
  - macOS Catalina (10.15)
  - macOS Big Sur (11.x)
- The following virtualization platforms are supported:
  - VMware Workstation 16 Pro
  - VMware Workstation 15 Pro
  - Microsoft Hyper-V Server 2012 64-bit
  - Microsoft Hyper-V Server 2012 R2 64-bit
  - Microsoft Hyper-V Server 2016 64-bit
  - Microsoft Hyper-V Server 2019 64-bit
  - Citrix XenServer 7.1 LTSR
  - Citrix XenServer 8.x
  - VMware vSphere 7.1
  - VMware vSphere 6.7

1.4 TOE Description

11 This section addresses the physical and logical components of the TOE that are included in the evaluation.

1.4.1 Physical scope

12 General overview of physical scope is shown in Figure 1.

13 The TOE physical boundary is restricted to the TOE application modules installed on the devices' operating systems in the evaluated configuration.

14 The installation package is delivered as a binary installation package:

15 ksc_13_13.0.0.11247_full_en.exe with size 457 460 632 bytes and the SHA256 checksum 42210DB5E9F5EFE9A18E9B8F3C4BC7CF71433BBB844C1F6170586243B8370B27.

16 The following documents are delivered as installation, administration and operational guidance to the end user and also considered to be a part of the TOE:

17 “Kaspersky Security Center. User Manual” version 2.00 as a PDF file with the SHA256 checksum 27C4FCD9C24EA8835C964F18C43DC03D491F711B2F5B0A7F34C6E11FD0BE968B.

18 “Kaspersky Security Center. User Manual. Addendum A” version 2.02 as a PDF file with the SHA256 checksum 5667972B31C2F58537B584478F201FF1E97FA6BCCA99FDEC001B097F31412E6C.

19 “Kaspersky Security Center. Preparative procedures” version 2.02 as a PDF file with the SHA256 checksum DFBB230939D34B6667CEE67D7F75B7F9DE32BE59B00391218CCB46D0A84D0A11.

20 The delivery of the TOE is secured in a manner that any user is able to determine the authenticity of the software package received. The delivery package, including the TOE and associated documentation is downloaded from Kaspersky Lab website

21 All executable files of the TOE, including installation package, are digitally signed with a Code Signing Certificate with a timestamp. This allows customers to verify the origin, integrity and authenticity of the TOE. The installation guide delivered together with the product explains how to securely install and configure product in order to bring it into the evaluated state. Also, the SHA256 checksums of the TOE binary files are provided to the customers to confirm that the received TOE files are the expected ones.

1.4.2 Evaluated configuration

22 The product was evaluated in the following configuration (see Figure 2):

- Administration Server is installed on a device running Windows Server 2016 Standard (LTSB) 64-bit.
- MySQL 5.7 64-bit is installed on the same device as Administration Server.
- Web Console is installed on a device running Windows 10 Education (20H2) 64-bit.
- Network Agent is installed on a managed endpoint device running Windows 10 Education (20H2) 64-bit.
- Managed endpoint device also has Kaspersky Endpoint Security for Windows (version 11.6.0.394 AES256) installed.
- All devices connected to LAN.

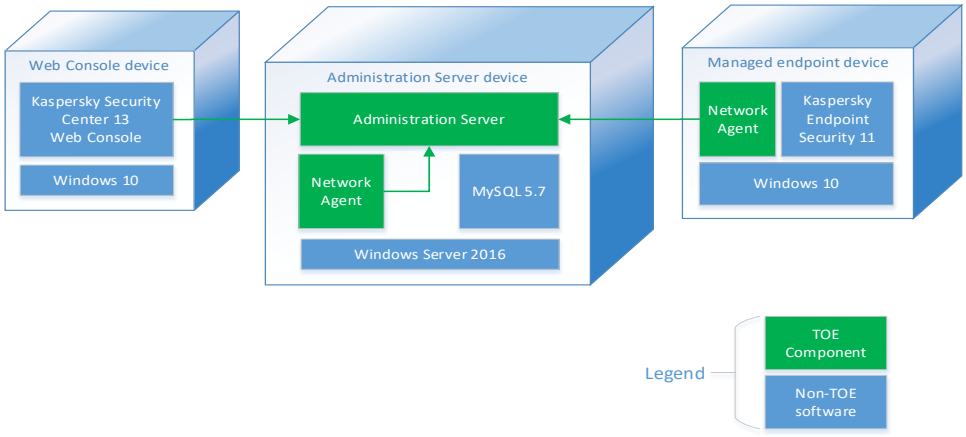

Figure 2. Evaluated configuration

1.4.3 Logical scope

23 The TOE logical scope consists of the following security functionality.

1.4.3.1 Audit

24 The TOE generates audit trail of events related to the TOE functioning and management, together with audit events received from managed AV applications (AV applications are outside of the TOE evaluation scope).
25 The TOE is able to read audited events from audit trail and extract them for users' review.
26 The TOE is able to control access to audited events depending on the user's role.

1.4.3.2 Protected communication

27 The TOE protects TSF data in transit between the TOE parts with the use of cryptographic functions. The distribution of installation packages is not part of the TOE. Any installation packages created with the help of the TOE are out of scope of the TOE security functionality.
28 The TOE generates cryptographic keys in accordance with a specified cryptographic key generation algorithm and specified cryptographic key sizes that meet the specified standards.
29 The TOE destroys cryptographic keys in accordance with a specified cryptographic key destruction method.
30 The TOE performs cryptographic operations in accordance with a specified cryptographic algorithm and cryptographic key sizes that meet the specified standards.

1.4.3.3 Administration

31 The TOE requires users to be successfully identified and authenticated before allowing access to its functions.
32 The TOE provides management functions for authorised administrative roles and restricts management of the TSF attributes for low-privileged roles and unauthorised users.
33 The TOE is able to associate authenticated users with roles.
34 The TOE enforces the access control policies over KSC objects belonging to the following groups:

- Monitoring & Reporting
- Devices
- Users & Roles
- Discovery & Deployment
- Operations.

2 Conformance Claims

2.1 CC Conformance Claim

35 This Security Target and the TOE claim conformance to part 2 and part 3 of CC Version 3.1, Revision 5:
36 CC part 2 conformant.
37 CC part 3 conformant.

2.2 PP Claim

38 This Security Target does not claim conformance to a Protection Profile.

2.3 Package Claim

39 This Security Target claims conformance to EAL2 augmented with ALC_FLR.1 [CCp3].

2.4 Conformance Rationale

40 As this Security Target does not claim conformance to a Protection Profile a conformance claim rationale is not necessary.

3 Security Problem Definition

41 This section defines the security problem to be addressed by the TOE and its operational environment.

3.1 Assets

42 Assets that are being secured by the TOE are specified in table below.

Name	Description
ASS.TOE_DATA	The TOE settings, including secure configuration and system-specific settings that are stored in files and registry, and/or the TOE data that are generated during TSF operation and are required for their correct functioning. Any installation packages created with the help of the TOE are not considered to be TOE data.
ASS.ENDPOINT_DATA	Data that are retrieved from managed endpoint and managed anti-virus application and is being processed, transferred and presented to the users.

43 Confidentiality and integrity of these assets are the values to be protected.

3.2 Threats

44 Threats are defined by an adverse action performed by a threat agent on an asset.

45 Threat agents may be:

- (1) Unauthorised users, processes or external entities. They have public knowledge of how the TOE operates and are assumed to possess a basic skill level and motivation commensurate with the attack potential defined by the EAL2 package. The threat agent may initiate a process within the TOE to act on its behalf. This threat agent can be any user (or process) of the operational environment of the TOE, or any user (or process) of devices connected to the organization's LAN, except for respective administrators. This threat agent has no authorised access to the TOE.
- (2) Authenticated users, that have an assigned role with limited rights in the TOE. This threat agent can be any user of the TOE, except for administrators. This threat agent has an authorised limited access to the TOE.

46 **Threats** are specified in the following table:

Name	Description
T.UNAUTHORISED_ACCESS	A threat agent (1) may wish to gain access to ASS.ENDPOINT_DATA when in transit between Network Agent and Administration Server by intercepting traffic. A threat agent (2) when authenticated with the TOE may wish to gain access to ASS.TOE_DATA and ASS.ENDPOINT_DATA, that they have no rights to access.
T.FORGERY	A threat agent (1) may wish to modify ASS.TOE_DATA and ASS.ENDPOINT_DATA when in transit between Network Agent and Administration Server.

3.3 Organizational Security Policies

47 An Organizational Security Policy is a set of security rules, procedures, or guidelines imposed by an organization on the operational environment of the TOE.

Name	Description
P.AUDIT	The TOE shall generate an audit record of auditable events and prevent unauthorised modification of the audit trail, and provide authorised users with the ability to review the audit trail.
P.ADMINISTRATION_ ACCESS	The TOE shall provide mechanisms to ensure that only administrators are able configure all functions of the TOE.

3.4 Assumptions

48 This section describes the security aspects of the intended environment for the evaluated the TOE. The operational environment must be managed in accordance with assurance requirement documentation for delivery, operation, and user guidance.

Name	Description
A.PHYSICAL	It is assumed that physical security is provided by the environment so that the TOE is not physically accessible for unauthorised users.
A.TRUSTED_ ADMIN	It is assumed that users with administrative privileges for the TOE (those with access to Basic functionality[4] of Administration Console) and administrators of underlying operating system are trusted to follow and apply all administrator guidance in a trusted manner and will not attempt to compromise the TOE and/or system security.
A.TRUSTED_ PLATFORM	The TOE relies upon a trustworthy computing platform for its execution. This includes the underlying platform and whatever runtime environment it provides to the TOE. It is assumed that RDBMS, where the collected data are stored, is deployed in a secure location and no unauthorised access to it is possible.
A.TIMESTAMP	It is assumed that the IT environment provides the TOE with the necessary reliable timestamps.

[4] As defined in “Kaspersky Security Center. User Manual” version 2.00 (the ‘Kaspersky Security Center licensing options’ chapter).

4 Security Objectives

4.1 Security Objectives for the TOE

49 The security objectives for the TOE are specified in the following table:

Name	Description
O.TOE_ ADMINISTRATION	The TOE will provide mechanisms to ensure that only authorised users are able to log in with administrative privileges and configure all functions of the TOE.
O.AUDIT	The TOE will generate an audit record of auditable events and prevent unauthorised modification of the audit trail, and provide the authorised users with the ability to review the audit trail.
O.PROTECTED_ COMMUNICATIONS	The TOE will provide protected communication channels (confidentiality, integrity and server identification) for remote administration, for authorised external IT entities, and for transfer of TSF data between the TOE parts.

4.2 Security Objectives for the operational environment

50 The security objectives for the operational environment are specified in the following table:

Name	Description
OE.PHYSICAL	Physical security is provided by the operational environment so that the TOE is not physically accessible for unauthorised users.
OE.TRUSTED_ ADMIN	Users with administrative privileges (administrators) for the TOE and the underlying operating system should follow and apply all administrator guidance in a trusted manner and should not attempt to compromise the TOE security.
OE.TRUSTED_ PLATFORM	The TOE relies upon a trustworthy computing platform for its execution. This includes the underlying platform and whatever runtime environment it provides to the TOE. RDBMS, where the collected data are stored, should be deployed in a secure location and no unauthorised access to it is possible.
OE. TIMESTAMP	The operational environment of the TOE must provide reliable timestamps to the TOE.

4.3 Security Objectives rationale

4.3.1 Security Objectives Coverage

51 The following table provides a mapping of security objectives for the TOE and the TOE environment to the defined threats, policies and assumptions, illustrating that each security objective for the TOE covers at least one threat or policy and that each security objective for the TOE environment covers at least one policy, threat or assumption.

Threat, Policy, or Assumption / Objective	T.UNAUTHORISED_ ACCESS	T.FORGERY	P.AUDIT	P.ADMINISTRATION_ ACCESS	A.PHYSICAL	A.TRUSTED_ADMIN	A.TRUSTED_ PLATFORM	A.TIMESTAMP
O.TOE_ADMINISTRATION	X			X				
O.AUDIT			X					
O.PROTECTED_COMMUNICATIONS	X	X						
OE.PHYSICAL					X			
OE.TRUSTED_ADMIN						X		
OE.TRUSTED_PLATFORM							X	
OE.TIMESTAMP								X

52 The following table shows why the chosen objectives are sufficient to counter a threat or satisfy an assumption.

Threat, Policy, or Assumption	Objectives
T.UNAUTHORISED_ ACCESS	O.TOE_ADMINISTRATION will provide mechanisms to ensure that only authorised users are able to log in with administrative privileges and configure all functions of the TOE. O.PROTECTED_COMMUNICATIONS provide protected communication channels (confidentiality, integrity and server identification) for remote administration, for authorised external IT entities, and for transfer of TSF data between the TOE parts, mitigating this threat by means of this channel confidentiality and prevents unauthorised access to assets through communication intercept.
T.FORGERY	O.PROTECTED_COMMUNICATIONS provides protected communication channels (confidentiality, integrity and server identification) for remote administration, for authorised external IT entities, and for transfer of TSF data between the TOE parts, mitigating this threat and prevents data forgery in transit by ensuring communication channel integrity and prevents attacker from impersonalizing the TOE through server identification.
P.AUDIT	O.AUDIT provides audit record of auditable events and prevent unauthorised modification of the audit trail, and provide the authorised users with the ability to review the audit trail.
P.ADMINISTRATION_ ACCESS	O.TOE_ADMINISTRATION will provide mechanisms to ensure that only authorised users are able to log in with administrative privileges and configure all functions of the TOE.
A.PHYSICAL	OE.PHYSICAL directly upholds this assumption.
A.TRUSTED_ADMIN	OE.TRUSTED_ADMIN directly upholds this assumption.
A.TRUSTED_PLATFORM	OE.TRUSTED_PLATFORM directly upholds this assumption.
A.TIMESTAMP	OE.TIMESTAMP directly upholds this assumption.

5 Extended components definition

53 No extended components defined.

6 Security Requirements

54 The CC allows several operations to be performed on functional requirements; refinement, selection, assignment and iteration are defined in Section 8.1 of Part 1 of the CC.

55 The notation, formatting and conventions used in this section are the following:

- Refinements are indicated by word '*Refinement*:' preceding the refined requirement, the refinement text coloured blue.
- Selections are enclosed in square brackets, i.g. [*selection*: result of selection], all coloured blue.
- Assignments are enclosed in square brackets, i.g. [*assignment*: result of assignment], all coloured blue.
- Iterations are indicated by forward slash symbol (/) followed by iteration name in capital letters, i.g. FMT_MSA.1/ADMIN.

6.1 TOE Security Functional Requirements

56 The following table summarises the list of SFRs implemented by the TOE.

Table 1. List of SFRs

SFR	SFR name
Security Audit	
FAU_GEN.1	Audit data generation
FAU_SAR.1	Audit review
FAU_SAR.3	Selectable audit review
FAU_STG.1	Protected audit trail storage
Cryptographic Support	
FCS_CKM.1	Cryptographic key generation
FCS_CKM.4	Cryptographic key destruction
FCS_COP.1	Cryptographic operation
Identification and Authentication	
FIA_UID.2	User identification before any action
FIA_UAU.2	User authentication before any action
FIA_SOS.1	Verification of secrets
FIA_AFL.1	Authentication failure handling
User Data Protection	
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
Security Management	
FMT_SMF.1	Specification of management functions

FMT_SMR.1	Security management roles
FMT_MSA.3	Static attribute initialization
FMT_MSA.1/ADMIN	Management of security attributes
FMT_MSA.1/OTHERS	Management of security attributes
Protection of the TSF	
FPT_ITT.1	Basic internal TSF data transfer protection

6.1.1 Class FAU: Security Audit

6.1.1.1 FAU_GEN.1 Audit data generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the [*selection, choose one of*: not specified] level of audit; and

c) [*assignment*: events from the following table:

Component	Event
FIA_UID.2, FIA_UAU.2	All connections to the Administration Server
FMT_SMF.1	Objects modifications

].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*assignment:* none].

Application note: The outcome of the events is expressed by their Severity level: success corresponds to Info or Warning, and failure corresponds to Critical or Functional Failure.

6.1.1.2 FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide [*assignment:* all predefined roles except for Self Service Portal User] with the capability to read [*assignment:* all information] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

6.1.1.3 FAU_SAR.3 Selectable audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply [*assignment*: sorting, ordering] of audit data based on [*assignment*: sorting by field:

- Time
- Device
- Event

- Description
- Administration group
- Application
- Version
- Severity level
- Task
- Event registered
- Name of Virtual Administration Server

and sorting order:

- Ascending
- Descending].

6.1.1.4 FAU_STG.1 Protected audit trail storage

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to [*selection, choose one of*: prevent] unauthorised modifications to the stored audit records in the audit trail.

6.1.2 Class FCS: Cryptographic Support

6.1.2.1 FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1 *Refinement:* The TSF shall generate asymmetric cryptographic keys in accordance with a specified cryptographic key generation algorithm [*assignment*: RSA schemes] and specified cryptographic key sizes [*assignment*: 2048-bit] that meet the following: [*assignment:* FIPS 186-4, Appendix B.3].

Application note: This SFR addresses the key generation method for the establishment of trusted channels for remote administration and/or communications with Network Agents on endpoint devices.

The TSF implements TLS 1.2 with the cipher suites:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (preferred)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA.

6.1.2.2 FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*assignment*: overwrite with zeros] that meets the following: [*assignment*: none].

6.1.2.3 FCS_COP.1 Cryptographic operation

FCS_COP.1.1 The TSF shall perform [*assignment*: encryption and decryption] in accordance with a specified cryptographic algorithm [*assignment:* AES] and cryptographic key sizes [*assignment:* 128-bit, 256-bit] that meet the following: [*assignment:* NIST SP 800-38D].

Application note: This SFR addresses the cryptographic operations performed for the establishment of trusted channels for remote administration and/or communications with Network Agents on endpoint devices.

The TSF implements TLS 1.2 with the cipher suites:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (preferred)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA.

6.1.3 Class FIA: Identification and Authentication

57 These SFRs refer to the Identification and Authentication for the administration of the TOE via web interface (Open API).

6.1.3.1 FIA_UID.2 User identification before any action

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.1.3.2 FIA_UAU.2 User authentication before any action

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.1.3.3 FIA_SOS.1 Verification of secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [*assignment*: following password policy:

a) Characters allowed:

- A – Z
- a – z
- 0 – 9
- @ # $ % ^ & * - _ ! + = [ ] { } | \ : ' , . ? / ` ~ " ( ) ;

b) Characters disallowed:

- Unicode characters

- spaces
- Cannot contain a dot character '.' immediately preceding the '@' symbol

c) Password restrictions:

- 8 characters minimum and 16 characters maximum
- Must contain characters at least from any 3 of 4 groups mentioned in the section “Characters allowed”].

Application note: This SFR refers to the secrets of the internal users of the TOE only. The secrets of the operating system users are maintained by operating system itself.

6.1.3.4 FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when [*selection: assignment:* 10] unsuccessful authentication attempts occur related to [*assignment:* authentication attempts of internal users of the TOE].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [*selection*: met], the TSF shall [*assignment*: forbid authentication attempts for this account for 1 hour].

Application note: This SFR refers to web interface (Open API) authentication. The lock for local system users or for domain users is defined by local/domain password policies, which are set by system administrator.

6.1.4 Class FDP: User Data Protection

58 This class SFRs refer to access control for the TOE administration.

6.1.4.1 FDP_ACC.1 Subset access control

FDP_ACC.1.1 The TSF shall enforce the [*assignment*: Administration SFP] on [*assignment*:

- Subjects: authenticated users;
- Objects: Administration Server objects;
- Operations among subjects and objects covered by the SFP: read, write and execute].

Application note: “Administration Server objects” are the administration functions accessible from the administration console groups:

- Monitoring & Reporting
- Devices
- Users & Roles
- Discovery & Deployment
- Operations.

6.1.4.2 FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the [*assignment*: Administration SFP] to objects based on the following: [*assignment*:

- Subjects: authenticated users. Attributes: user identity and role.
- Objects: Administration Server objects. Attributes: object identifier].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*assignment*:

- A subject is allowed to perform an operation on an object only if the subject's role has rights allowing that operation on that object].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*assignment*:

- Main Administrator role is granted all access rights to all objects.
- Main Operator role is granted rights to read and execute all objects].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*assignment*: none].

Application note: "Administration Server objects" are the administration functions accessible from the administration console groups:

- Monitoring & Reporting
- Devices
- Users & Roles
- Discovery & Deployment
- Operations.

6.1.5 Class FMT: Security Management

6.1.5.1 FMT_SMF.1 Specification of management functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [*assignment*:

- Users management;
- Security rights management;
- Audit events settings].

6.1.5.2 FMT_SMR.1 Security management roles

FMT_SMR.1.1 The TSF shall maintain the roles [*assignment*:

- Administration Server Administrator
- Administration Server Operator
- Auditor
- Installation Administrator
- Installation Operator
- Kaspersky Endpoint Security Administrator
- Kaspersky Endpoint Security Operator
- Main Administrator
- Main Operator
- Mobile Device Management Administrator
- Mobile Device Management Operator
- Security Officer
- Self Service Portal User
- Supervisor
- Vulnerability and Patch Management Administrator
- Vulnerability and Patch Management Operator
- optional custom configurable roles].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

Application note: During KSC deployment two OS user groups are created: KLAdmins, to which assigned the Main Administrator role, and KLOperators, to which assigned the Main Operator role. By default, to OS administrators also assigned the Main Administrator role. To other users their roles can be assigned explicitly.

6.1.5.3 FMT_MSA.3 Static attribute initialization

FMT_MSA.3.1 The TSF shall enforce the [*assignment*: Administration SFP] to provide [*selection, choose one of*: restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [*assignment*: Main Administrator role] to specify alternative initial values to override the default values when an object or information is created.

Application note: The rights granted by default to predefined roles cannot be modified.

6.1.5.4 FMT_MSA.1/ADMIN Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the [*assignment*: Administration SFP] to restrict the ability to [*selection*: query, modify, delete, [*assignment*: view]] the security attributes [*assignment*: subjects and objects' attributes governing the "Administration SFP"] to [*assignment*: users with Main Administrator role or other roles that have rights allowing listed operations on the security attributes].

Application note: The rights granted by default to predefined roles cannot be modified.

6.1.5.5 FMT_MSA.1/OTHERS Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the [*assignment*: Administration SFP] to restrict the ability to [*selection*: query] the security attributes [*assignment*: subjects and objects' attributes governing the "Administration SFP"] to [*assignment*: users with Main Operator role or other roles that have rights allowing query operation on the security attributes].

Application note: The rights granted by default to predefined roles cannot be modified.

6.1.6 Class FPT: Protection of the TSF

6.1.6.1 FPT_ITT.1 Basic internal TSF data transfer protection

FPT_ITT.1.1 The TSF shall protect TSF data from [*selection*: modification] when it is transmitted between separate parts of the TOE.

6.1.7 Rationale for Security Functional Requirements

59 The following table maps security objectives to security functional requirements, showing that each security objective is covered by at least one security functional requirement and that no security functional requirement exists that is not needed by any security objective.

SFR	O.TOE_ ADMINISTRATION	O.AUDIT	O.PROTECTED_ COMMUNICATIONS
FAU_GEN.1		X	
FAU_SAR.1		X	
FAU_SAR.3		X	
FAU_STG.1		X	
FCS_CKM.1			X
FCS_CKM.4			X
FCS_COP.1			X
FIA_UID.2	X		
FIA_UAU.2	X		
FIA_SOS.1	X		
FIA_AFL.1	X		

SFR	O.TOE_ ADMINISTRATION	O.AUDIT	O.PROTECTED_ COMMUNICATIONS
FDP_ACC.1	X	X	
FDP_ACF.1	X	X	
FMT_SMF.1	X		
FMT_SMR.1	X		
FMT_MSA.3	X		
FMT_MSA.1/ ADMIN	X		
FMT_MSA.1/ OTHERS	X		
FPT_ITT.1			X

60 The following table shows what the individual security functional requirements contribute to the objective and that the requirements are sufficient to satisfy the objective.

Objective	Requirements
O.TOE_ ADMINISTRATION	FIA_UID.2 ensures users are identified before access to the TOE data. FIA_UAU.2 ensures users are authenticated before access to the TOE data. FIA_SOS.1 ensures authentication secrets are complex. FIA_AFL.1 ensures authentication brute-force attack is unpractical. FDP_ACC.1 ensures access to the TOE data is controlled. FDP_ACF.1 ensures access to the TOE data is controlled by rules. FMT_SMF.1 ensures the TOE management. FMT_SMR.1 ensures the TOE support access roles. FMT_MSA.3 ensures initialization of security attributes. FMT_MSA.1/ADMIN ensures management of security attributes. FMT_MSA.1/OTHERS ensures management of security attributes.
O.AUDIT	FAU_GEN.1 ensures audit data are being generated. FAU_SAR.1 ensures audit data can be reviewed. FAU_SAR.3 ensures audit data can be review with selection. FAU_STG.1 ensures audit data are protected from unauthorised deletion. FDP_ACC.1 ensures access to audit data is controlled. FDP_ACF.1 ensures access to audit data is controlled by rules.

O.PROTECTED_ COMMUNICATIONS	FCS_COP.1 ensures the data encryption/decryption with the keys generated as defined in FCS_CKM.1 when implementing FPT_ITT.1 FCS_CKM.1 ensures correct key generation. FCS_CKM.4 ensures that keys are destroyed in a safe way. FPT_ITT.1 ensures communication is protected.

6.1.8 Security Functional Requirements Dependency Analysis

61 All dependencies of the SFRs are summarised in following table:

SFR	Dependencies required by [CCp2]	Dependencies are met by
FAU_GEN.1	FPT_STM.1	OE.TIMESTAMP
FAU_SAR. 1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.3	FAU_SAR.1	FAU_SAR.1
FAU_STG.1	FAU_GEN.1	FAU_GEN.1
FCS_CKM.1	FCS_CKM.2 or FCS_COP.1, FCS_CKM4.	FCS_COP.1, FCS_CKM4.
FCS_CKM.4	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	FCS_CKM.1
FCS_COP.1	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4	FCS_CKM.1, FCS_CKM.4
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1, FMT_MSA.3
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1, FMT_SMR.1, FMT_SMF.1	FDP_ACC.1, FMT_SMR.1, FMT_SMF.1
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	FMT_MSA.1, FMT_SMR.1
FMT_SMR.1	FIA_UID.1	FIA_UID.2
FIA_UAU.2	FIA_UID.1	FIA_UID.2
FIA_AFL.1	FIA_UAU.1	FIA_UAU.2

62 The table above demonstrates that all dependencies are either satisfied by an SFR or an operational environment objective.

6.2 Security Assurance Requirements

63 The security assurance requirements for the TOE are EAL2 augmented with ALC_FLR.1 component as specified in [CCp3].

6.2.1 Rationale for Security Assurance Requirements

64 EAL2 was chosen to provide a low to moderate level of assurance that is consistent with good commercial practices.

65 The TOE is expected to be operated in a non-hostile environment and is assumed to be protected for physical security and under specific non-it assumptions. At EAL2, the TOE is subjected to a vulnerability analysis with a “basic” attack potential supposed for possible attackers in the declared environment.

66 The augmentation of ALC_FLR.1 was chosen to give greater assurance of the developer’s flaw remediation processes.

6.2.2 Security Assurance Requirements Dependency Analysis

67 All dependencies of the SARs required by the [CCp3] have been satisfied. Since ALC_FLR.1 does not have dependencies and EAL2 satisfies its own dependencies, EAL2 augmented with ALC_FLR.1 is consistent with regard to its dependencies.

7 TOE Summary Specification

68 This section contains description of how the TOE meets all the SFRs. The following table helps associate SFR with relevant description.

Table 2. Mapping of SFRs to TSFs

SFR	SFR name	TSF
FAU_GEN.1	Audit data generation	Audit
FAU_SAR.1	Audit review	Audit
FAU_SAR.3	Selectable audit review	Audit
FAU_STG.1	Protected audit trail storage	Audit
FCS_CKM.1	Cryptographic key generation	Protected communications
FCS_CKM.4	Cryptographic key destruction	Protected communications
FCS_COP.1	Cryptographic Operation	Protected communications
FIA_UID.2	User identification before any action	Administration
FIA_UAU.2	User authentication before any action	Administration
FIA_SOS.1	Verification of secrets	Administration
FIA_AFL.1	Authentication failure handling	Administration
FDP_ACC.1	Subset access control	Administration
FDP_ACF.1	Security attribute based access control	Administration
FMT_SMF.1	Specification of management functions	Administration
FMT_SMR.1	Security management roles	Administration
FMT_MSA.1/ADMIN	Management of security attributes	Administration
FMT_MSA.1/OTHERS	Management of security attributes	Administration
FMT_MSA.3	Static attribute initialization	Administration
FPT_ITT.1	Basic internal TSF data transfer protection	Protected communications

7.1 Audit

69 The TOE generates audit records related to the TOE activity, together with records generated by managed AV applications as per **FAU_GEN.1**. The TOE stores the generated events in RDBMS. Users can access these records from RDBMS via web interface, which satisfies **FAU_SAR.1.** Users can apply selection criteria to audit records by creating customised report in web interface (Open API), which this satisfies **FAU_SAR.3**.

70 Only authorised access to audit records is allowed by the TOE, satisfying **FAU_STG.1**.

7.2 Administration

71 The TOE provides administration capabilities to authorised users via web interface (Open API) (for facilitation one can use Kaspersky Security Center 11 Web Console (not a part of the TOE)) and command line utilities.

72 Administration functionality includes role-based access control to the TOE data and the TOE management, restricting access of viewing (‘read’ operation), modifying (‘write’ operation), or executing (‘execute’ operation) of the TOE data objects (such as tasks or audit reports) or their security attributes (settings) according to access rights of users requesting this access as per **FMT_MSA.1/ADMIN, FMT_MSA.1/OTHERS, FMT_MSA.3** requirements.

73 The TOE data related to AV infrastructure includes objects belonging to the following groups:

- Monitoring & Reporting
- Devices
- Users & Roles
- Discovery & Deployment
- Operations.

74 The TOE as per **FMT_SMF.1** provides management of following functions:

- Users management;
- Security rights management;
- Audit events settings.

75 These also can be done through web interface.

76 To satisfy **FMT_SMR.1** the TOE provides two main predefined access roles: Main Administrator and Main Operator, and other predefined roles which can be assigned to other users when and if needed.

77 By default, OS users that belong to the KLAdmins group have Main Administrator role, while KLOperators group users have Main Operator role. The KLAdmins and KLOperators groups are created automatically in the OS during the TOE installation.

78 Moreover, there can be added other configurable roles with specific configuration of access rights.

79 Access to the TOE data and management functions is granted based on subject access role, so **FDP_ACC.1** and **FDP_ACF.1** are satisfied.

80 The TOE satisfies **FIA_UID.2, FIA_UAU.2** by requiring user's identification and authentication before they will be allowed to take any action with the TOE via web interface (Open API). The TOE will ensure that internal KSC users' passwords are sufficiently complex, which satisfies **FIA_SOS.1.** The command line interfaces only accessible for authenticated OS users with administrator privileges on the Administration Server or managed endpoint devices.

81 The TOE satisfies **FIA_AFL.1** as it provides protection from brute-force attacks on user credentials by blocking attacked user account for an hour after 10 failed login attempts via web interface (Open API).

7.3 Protected communications

82 The TOE will generate encryption keys and certificates to protect communication between the TOE parts via protocol encryption. Keys are generated by the TOE, stored securely in protected data storage and destroyed when no longer needed, which satisfies **FCS_CKM.1**, **FCS_CKM.4**.

83 Communications between the separate TOE parts (Administration Server and Network Agent, located on different physical (or virtual) devices) are encrypted using TLS 1.2 protocol with certificate-based encryption, which satisfies **FCS_COP.1** If encryption handshake fails, the connection is terminated.

84 Communications between the TOE and external trusted entities that use Open API provided by KSC (including Web Console, which is not a part of the TOE) are also protected by TLS 1.2 encryption, which also satisfies **FCS_COP.1**. If encryption handshake fails, the connection is terminated.

85 Communications between the TOE parts are protected from modification, which satisfies **FPT_ITT.1**.

8 References

Reference	Document
[CCp1]	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017
[CCp2]	Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017
[CCp3]	Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components; CCMB-2017-04-003, Version 3.1, Revision 5, April 2017
[CEM]	Common Methodology for Information Technology Security Evaluation, CCMB-2017-04-004, Version 3.1, Revision 5, April 2017
[FIPS 186-4]	FIPS PUB 186-4, Digital Signature Standard (DSS) / National Institute of Standards and Technology (NIST), July 2013
[NIST SP 800-38D]	NIST Special Publication 800-38D, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC / National Institute of Standards and Technology (NIST), November 2007

kaspersky

www.kaspersky.com/
www.securelist.com