kaspersky

Hard Disk & Removable Drive Encryption Service

Introduction

This document describes the Hard Disk and Removable Drive Encryption Service provided by our experts at Kaspersky.

The goal of the Hard Disk and Removable Drive Encryption Service is to implement disk and file encryption effectively and to your complete satisfaction in your environment, within the scope of work agreed.

Coverage

Up to 20 disks and\or 20 files

Service timeline

This service allows for a maximum of 8 labor hours to achieve this goal, and covers a maximum of 20 disks and 20 files. Once everything is fully delivered to your satisfaction, the project will be defined as ‘completed’, even if less than 8 labor hours have been used.

The service includes HDD, file & removable drive encryption, and can be divided into following stages:

Introduction	Encryption service	Finalization
Initial meeting to clarify the concept of encryption.	Configuration of authentication agent options and implementation of full disk encryption module. After configuration, computers will need to be rebooted.	Full encryption of HHD and removable drives, explanation of the further usage.
The prerequisite environment checks (remote access, results of the FDE test utility, network communications, and license).	Demonstration and instruction on: • how to manage authentication agent accounts through creating tasks. • how to set up a report to view authentication agent accounts. • the challenge response procedure • how to decrypt a disk and where to display the status. • the operational principles of file encryption. • file encryption rules in the policy	
Explanation of disk encryption specifications and how the authentication agent works. NB: You will need to back up your Kaspersky Security Center in advance – the labor hours included in this service do not allow enough time for our security experts to do this on your behalf.	• Implementation of file level encryption module (may include a computer reboot). • Demonstration of the use of encrypted packages and explanation of the types of encryption for removable drives. • File encryption and instructions on how to transfer encrypted files inside and outside the organization	

Requirements & further information

Please note that Kaspersky is under no obligation to deliver or attempt to deliver this service if the requirements listed below have not been fully met. Please let us know immediately should meeting any of these requirements present a potential problem.

1. The service is delivered remotely and can be divided in 2 'windows' of 4 hours each – you will need to agree this timing with us in advance.
2. The customer must provide access to their environment remotely using the Zoho Assist tool (TCP ports 80 and 443 only, see detailed requirements https://www.zoho.com/assist/kb/firewall-configuration.html)
3. A representative of your IT department or security team must be available at all times during service delivery to meet any reasonable request from our Kaspersky Engineers, including permissions, access, etc.
4. The environment must have Kaspersky Endpoint Security (Advanced license or above), Kaspersky Security Center and Kaspersky Network Agents already installed.
5. The server must meet the requirements of the current version of Kaspersky Security Center. For more information visit the following websites (please select your application version in the upper right corner of the pages provided below):
   a. Hardware and software requirements: https://support.kaspersky.com/KSC/14/en-US/96255.htm
   b. Accounts for work with the DBMS: https://support.kaspersky.com/KSC/14/en-US/156275.htm
   c. Ports used by Kaspersky Security Center: https://support.kaspersky.com/KSC/14/en-US/158830.htm
6. Remote access must be executed on all computers with installed Kaspersky Security Center installed as well as on each computer to be encrypted.
7. Computers must be available throughout service delivery for repeated reboots if necessary. Dual-boot and multi-OS environments are not supported for hard disk encryption;
8. Network agents must be able to communicate freely with Kaspersky Security Center.
9. The devices on which full disk encryption will be applied must pass the FDE utility test. For more information, visit https://support.kaspersky.com/14328;
10. The server on which Kaspersky Security Center is to be installed must have enough space to store the backup. For more information, visit https://support.kaspersky.com/10585#block3;
11. You must perform a backup of your Kaspersky Security Center installation before the start of service delivery (this is not included in the service and our Kaspersky experts won't have time to do this for you).
12. The policy that controls the devices to which encryption is to be applied must be correctly configured and applied.
13. The computers to which encryption is to be applied must be all be running a version of MS Windows operating system compatible with the version of Endpoint installed.
14. You must ensure that all Kaspersky products have been upgraded to the latest versions. "End of Life" or "Limited support" Kaspersky products are out of the scope of this service.

Please note that:

- Dual-boot and multi-OS environments are not supported for hard disk encryption
- Any failures that require analysis during implementation will be addressed through our support service

Scope of work

In Scope	Out of Scope
• Explain conceptually the usefulness of cryptography and applicable types of encryption in Kaspersky; • Implement full HDD disk, file and removable drives encryption with the activities determined in the Project Timeline session.	Our engineers are instructed only to work on tasks or products strictly associated with the delivery of our encryption service as defined by the scope and deliverables outlined here, unless otherwise agreed in advance. Examples of tasks that fall outside the of scope of this service are:

- The creation of any type of policy. The policy used for encryption will be a copy of the policy that you have created and use for protection.
- The integration of Kaspersky Security Center with Active Directory.
- The installation of any protection component - endpoint protection must already be installed and functional.
- The creation of customized reports.
- Troubleshooting any encryption incompatibilities. This type of problem must be resolved through reporting as an incident to the technical support team.
- The creation of users, DNS, DHCP, Active Directory or any other network services.
- Working with any products other than those provided by Kaspersky.
- Making backup copies of the machines or systems involved in the project.
- The installation of any operating system.

Outcome and Deliverables

Encryption will be implemented in your infrastructure for up to 20 disks and files. Your team will also know how to use product features, including how to use and manage encrypted disks and files.

Notes

Additional configurations, deployment and corrections can also be performed to meet your specific needs if required. Please ask your Account Manager to create a custom proposal for you. Such custom services should be purchased separately.

Our schedule of work will be based on the availability of the most appropriate Kaspersky resources, but work will start no longer than 15 days after we receive the go-ahead to start the project from you in writing.

kaspersky

www.kaspersky.com
Kaspersky Professional Services