kaspersky

Kaspersky Security Center Cloud Console Deployment

Introduction

This document describes the Kaspersky Security Center Cloud Console (KSC Cloud Console) deployment service provided by Kaspersky experts.

The goal of this service is to implement a simple protection architecture into your environment, through deploying a single KSC Cloud Console to manage Kaspersky Endpoint Security protection, which will be installed onto up to 5 endpoints.

Coverage

1(one) Kaspersky Security Center Cloud Console and up to 5 endpoints with Kaspersky Endpoint Security protection

Service timeline

NB. This service allows for a maximum of 8 labor hours to achieve this goal. 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 is divided into the following stages:

Introduction	Deployment	Finalisation
Kick off and explaining the architecture.	Registering the Kaspersky Security Center Cloud Console and adding the activation code. Accepting the EULA of the Kaspersky Network Agent installation package in the KSC Cloud Console.	Demonstrating how it works and talking your administrator through the process. (the link to the tutorial can be provided)
Conducting the prerequisite checks on your environment (remote access, network communications, internet access, server requirements).	Create 1 or 2 groups of protected devices.	Creating a Completion Report
	Creating a Network Agent and Endpoint policies for workstations.	
	Carrying out Update, Full Scan and Quick Scan tasks.	
	Downloading the standalone Network Agent installation package onto KSC Cloud Console. Installing the Network Agent onto the computer that is to act as the distribution point, and ensuring it communicates with the console.	
	Deploying the distribution point and configuring polling for the discovery of other devices.	
	Creating and configuring Kaspersky Endpoint Security packages.	
	Running the installation tasks for the Network Agent, and for Kaspersky Endpoint Security, on up to 5 endpoints.	

Requirements & statements

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.

- The service will be delivered remotely and can be divided into two ‘windows’ of four hours each. You’ll need to agree this timing with us in advance.
- The general architecture of KSC Cloud Console can be viewed at https://support.kaspersky.com/KESB/13.2/en-US/198657.htm
- You must provide access to your 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
- 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.
- Remote access must be executed on the computer with the connection to KSC Cloud Console.
- Your OS must be compatible with Kaspersky Endpoint Security Cloud Console. To confirm this, please visit:
  - https://help.kaspersky.com/KSC/CloudConsole/en-US/172903.htm
  - https://support.kaspersky.com/KESWin/11.10.0/en-US/127972.htm
- In order to access your KSC Cloud Console, you’ll need to add *.ksc.kaspersky.com as an exclusion in your firewall.
- Your nominated distribution point must have at least enough free disk space to easily accommodate the installation of all the necessary packages. For more information on the volume of space required, please visit: https://help.kaspersky.com/KSC/CloudConsole/en-US/98876.htm
- You must license for Kaspersky Endpoint Security Select, or Kaspersky Endpoint Security Advanced, or Kaspersky EDR Optimum licenses (purchased for at least 300 devices)
- Any security product installed on the target machines will need to be removed. If this doesn’t happen automatically, and if passwords or scripts for removing this and any other third-party software are not available, it will be your responsibility to remove any such software in advance. If necessary, we can create a separate support incident to handle this task, which will then need to be completed prior to the delivery of this service.
- We’ll be creating a structure based on a single site with default configuration.
- We’ll deploy onto up to 5 machines and we’ll share the knowledge with your administrators so that they can carry out deployment to the rest of your environment. Please note that the upper limit for KSC Cloud Console management is 10,000 devices.
- Any technical issues arising during deployment will addressed through our support service.

In Scope	Out of Scope
• Create a package for Kaspersky Endpoint Security • Create a package for Kaspersky Network Agent • Create a Policy for Kaspersky Endpoint Security and Kaspersky Network Agent • Create a task to update Kaspersky Endpoint Security across the environment • Create 1-2 groups for protected devices • Create a task to perform a Quick Scan and Full Scan on the environment • Install Kaspersky Network Agent on up to 5 machines	Kaspersky will not work on any task or product not explicitly described here under ‘In Scope’ & ‘Deliverables’. This includes: • Creating a secondary Kaspersky Security Center node on-site • Creating exclusions for applications not working with Kaspersky protection • Installing protection on Linux or Mac machines, or on mobile phones or tablets. • Deploying MDM features

- Install Kaspersky Endpoint Security on up to 5 machines
- Remove incompatible 3rd party security application if we have the files to do so. In case of an absence of files, a support incident will be created to handle this task and will be delivered after project completion
- Create a Report of Completion.

- Deploying Kaspersky Endpoint Encryption or Vulnerability Assessment and Patch Management modules.
- Configuring synchronization with SIEM systems.
- Handling user creations, DNS, DHCP, Active Directory or any other network services.
- Creating or editing rules for external firewalls or routers.
- Creating or editing any hypervisor environment.
- Performing backups from machines or systems involved in the project.
- Installing any operating system.

Outcome and deliverables

1. Kaspersky Security Center Cloud Console will be fully deployed and in operation.
2. Kaspersky Endpoint Security will be deployed on up to 5 workstations.
3. Your administrator will understand how to manage your endpoint security through the Kaspersky Security Center Cloud Console, and how to deploy your Kaspersky Endpoint Security onto further workstations, now and in future.
4. You will receive a Completion Report.

Notes

We can perform additional configurations and deployments, and many other tasks that fall outside the scope of our off-the-shelf services, through our custom Professional Services portfolio.   Please speak to your Account Manager about creating a custom proposal for you.

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.com
Kaspersky Professional Services