kaspersky

Kaspersky Security for Virtualization Light Agent Deployment Services Package

kaspersky

Introduction

This document describes Kaspersky Security for Virtualization Light deployment service provided by our experts at Kaspersky.

The goal of this service is to deploy Kaspersky Security for Virtualization Light Agent onto up to 10 endpoints, to your complete satisfaction, within the scope of work agreed.

Coverage

Up to 10 machines with Kaspersky Security for Virtualization Light Agent installed

Service timeline

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 Project can be divided into 3 stages:

<table>
<tr><th>Introduction</th><th>Deployment</th><th>Finalisation</th></tr>
<tr><td>Kick-off and talking through the architecture.</td><td>Installing Virtualization Administration Components.</td><td rowspan="8">Creating and delivering a Completion Report.</td></tr>
<tr><td rowspan="7">Checking through your systems architecture and environment (establishing remote access, validating binaries, looking at server patching, network communications, internet access, server requirements and validation keys).

.</td><td>Creating the following:
Administration Groups.
A policy for Protection Server(s).
A relocation rule for Protection Server and Light Agent.</td></tr>
<tr><td>Installing the Protection Server (up to 2 virtual machines)</td></tr>
<tr><td>Creating and configuring an update task, and then an activation task, for the Protection Server.</td></tr>
<tr><td>Running both activation and update tasks on the server and ensuring they run with no issues.</td></tr>
<tr><td>Creating:
A virus scan task for Light Agent for Windows.
A protection policy for Light Agents for Windows.
An installation package for Light Agents.</td></tr>
<tr><td>Installing light Agents onto Microsoft Windows Machines.</td></tr>
</table>

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.

- 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.
- Kaspersky Security Center should be already implemented on your system. If this could be an issue, please note that we also offer a separate Service Package for Kaspersky Security Center deployment.
- You will need to have already purchased all the licenses need for activation
- 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, including your domain and network administrators, must be available at all times during service delivery to meet any reasonable request from our Kaspersky Engineers, including permissions, access, etc.
- We’ll be installing the application in an infrastructure managed by a VMware vCenter Server and VMware NSX Manager, you need to configure the connection of the Integration Server with VMware NSX Manager as detailed in https://help.kaspersky.com/KSVLA/5.1/en-US/64729.htm;
- Kaspersky must have access without restrictions to the following:
  - The server where Kaspersky Security Center is installed.
  - The hypervisor where the Protection Server will be deployed.
- The Kaspersky Security Center server must be running the latest version, and must be up to date. For more information visit the following websites:
  - Hardware and software requirements: https://support.kaspersky.com/KSC/14/en-US/96255.htm
  - Accounts for work with the DBMS: https://support.kaspersky.com/KSC/14/en-US/156275.htm
  - Ports used by Kaspersky Security Center: https://support.kaspersky.com/KSC/14/en-US/158830.htm
- In addition, both Kaspersky Security Center and the Protection Server should have their ports open as described in https://support.kaspersky.com/KSVLA/5.2/en-US/133882.htm
- The hypervisor should have accounts privileges has detailed in https://support.kaspersky.com/KSVLA/5.2/en-US/85889.htm
- There are some specific conditions that your hypervisor must meet. For details, see: https://support.kaspersky.com/KSVLA/5.2/en-US/67424.htm
- The files required for installation should be downloaded onto the server. For more information, see https://support.kaspersky.com/ksv5la#downloads;
- Hardware and Software specifications should be as given at https://support.kaspersky.com/KSVLA/5.2/en-US/64743.htm
- Kaspersky Security Center server must have access to the internet without any restrictions, in order to perform downloads from the Kaspersky database.
- Any security product installed on the target machines should be removed. If this does not happen automatically, and if passwords or scripts for removing this and any other third-party software cannot be made available to us, 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 would then be delivered after project completion.
- We will deploy a Light Agent onto up to 50 machines, and we’ll show you how to perform this task for further machines in your environment.

Scope of work

In Scope	Out of Scope
• Install Integration server components. • Create a policy for the Protection Server and Light Agents. • Create Activation, Update and Scan tasks. • Create an installation package for Kaspersky Security for Virtualization Light Agent for Windows. • Create groups for the Protection Server and Light Agents.	• Non-persistent virtual machines will not be deployed • Linux machines will not be deployed • We will not work in any other task or product not explicitly described in “In Scope & Deliverables” sector, including • Performing any detection tests. Configuring the sending events to a SIEM system.

- Install and configure the Protection Server.
- Install the light agent onto up to 50 devices.
- Ensure that communications between the Light Agents, Protection Server and Integration Server are fully effective.
- Activate and update the product database.
- Remove any incompatible 3rd party security application if we have the files to do this. If we don't have these files, a support incident will be created to handle this task and will be delivered after project completion/
- Create and deliver a Completion Report.

- Creating kind of cluster or high availability.
- Creating exclusions for applications not working with Kaspersky protection.
- Installing protection in Mac machines, mobile phones and tablets.
- Deploy features for MDM, endpoint encryption or patch management.
- Handling user creations, DNS, DHCP, Active Directory or any other network services.
- Creating or editing rules for External Firewalls or Routers.
- Performing backups from machines or systems involved on the project.
- Installing any operating system other than as necessary for Kaspersky Security for Virtualization Light Agent deployment.
- Installing or configuring any hardware equipment.

Outcome and deliverables

1. All Virtualization Administration Components will be installed.
2. Up to 2 Protection Servers will be deployed in your hypervisor.
3. Kaspersky Security for Virtualization Light Agent for Windows will be installed up to 50 devices.
4. Your administrator will know how to deploy Kaspersky Security for Virtualization Light Agent for Windows onto further devices, now and in future.
5. There will be fully operative communications between your Integration Server, Protection Server and Light Agents.
6. 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 Service Packages, through our custom Professional Services portfolio. Please speak to your Account Manager about creating a custom proposal for you if needed.

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.

www.kaspersky.com
Kaspersky Professional Services