

The Kaspersky logo, consisting of the word "kaspersky" in a bold, lowercase, sans-serif font. The logo is positioned in the upper left corner of a white, irregularly shaped area that resembles a stylized shield or a piece of paper with rounded corners. The background of the entire image is a gradient of green, transitioning from a darker teal at the top to a lighter, vibrant green at the bottom.

kaspersky

Essential Installation Service for Kaspersky Unified Monitoring and Analysis Platform

Introduction

Kaspersky Professional Services is a set of services covering the complete product cycle, from assessment through implementation to maintenance and optimization.

Kaspersky SIEM (Kaspersky Unified Monitoring and Analysis Platform) is a next-generation solution designed to help your security team manage and analyze incoming security data. It excels at:

- Collecting, processing and storing events from diverse sources, including Kaspersky solutions, operating systems, third-party applications, security tools and databases.
- Analyzing and correlating incoming data in real time, enriching it with industry-leading Threat Intelligence to detect suspicious activity.
- Providing timely alerts to enable rapid incident investigation and response.
- Storing data for an extended period without exceeding the budget for costly storage hardware — thanks to hot and cold storage options with seamless simultaneous search functionality.

Integrating Kaspersky Unified Monitoring and Analysis Platform (hereinafter KUMA) with other products and systems enhances the efficiency of threat monitoring and response, as well as extends the protection scope.

This document describes the procedure and stages for providing the Essential installation and basic configuration of the Kaspersky Unified Monitoring and Analysis Platform service. The service is delivered by the Kaspersky Technical Support team.

The goal of this service is to have KUMA up and running in your environment within the scope of work agreed.

Coverage

One KUMA Server, connection to up to 10 event sources, integration with up to 3 Kaspersky solutions or infrastructure services.

Service timeline

This service allows for a maximum of 10 working days to achieve the goal. Once everything is fully delivered to your satisfaction, the project will be defined as 'completed', even if less than 10 working days have been used.

The service can be divided into the following stages:

- Kick-off meeting, check list completion and scope confirmation
- Sizing calculation
- Deployment and basic configuration
- Event sources connection
- Post-implementation

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.

The service is delivered remotely. To prepare and provide a deployment scenario, it is necessary to provide the data requested by Kaspersky engineers.

A representative of your IT department or security team must be available at all times during the service delivery to meet any reasonable request from our Kaspersky engineers, including permissions, access, etc.

The service is provided on current supported versions of KUMA, in accordance with the application lifecycle terms:

(<https://support.kaspersky.com/corporate/lifecycle?type=limited,full&program=kuma>)

Any technical issues arising during deployment will be addressed through our support service.

Scope of work

1. Sizing calculation (after receiving the questionnaire from the customer)
2. Deployment:
 - 2.1. Validation of hardware requirements based on sizing calculation (CPUs / RAM, disks)
 - 2.2. Verification of network connectivity between servers
 - 2.3. Configuration of DNS client and NTP client
 - 2.4. Operating system preparation (SSH key setup, sshd configuration, creation of logical volumes and mount points if necessary)
 - 2.5. Distribution of the installation package across servers (using kuma-ansible-installer)
 - 2.6. License activation
 - 2.7. Storage cluster installation
 - 2.8. Collector microservices installation (for pre-defined Standard sources)
 - 2.9. Correlator microservices installation
3. Integration with infrastructure services
 - 3.1. Domain authentication configuration (FreeIPA / Active Directory)
 - 3.2. Assignment of specific role permissions to AD groups
 - 3.3. Integration with an LDAP server (one server)
 - 3.4. Integration with an SMTP server
 - 3.5. Configuration of direct updates from the Kaspersky repositories (if direct Internet access is available; does NOT include additional deployment and configuration of KUU)
4. Post-implementation: knowledge transfer and summary report

Outcome and deliverables

KUMA will be deployed and configured, your administrator will know how to deploy KUMA and complete basic configuration. You will receive a Report of Completion.



Notes

We can perform additional configuration, deployment, and many other tasks that fall outside the scope of our off-the-shelf Service Packages, through our custom Professional Services portfolio. Please contact your Account Manager to discuss creating a custom proposal for you.

Examples of such services include:

- Integration of event sources, including standard ones
- Development of custom parsers for non-standard event sources
- Tuning and development of detection (correlation) rules
- Configuration of various response actions
- Custom reporting

Our schedule of work will be based on the availability of the most suitable Kaspersky resources, but work will start no later than 15 days after we receive your written approval to start the project.



www.kaspersky.com

© 2026 AO Kaspersky Lab.

All rights reserved. Registered trademarks and service marks are the property of their respective owners.