

Kaspersky[®] Private Security Network SaaSForce

Configuration Guide



The Cloud Services Provider

KA\$PER\$KYᡱ

Kaspersky Private Security Network • SaaSForce • Configuration Guide

This document guides you through the steps on how to connect to the KPSN (Kaspersky Private Security Network), which is facilitated by SaaSForce in the Netherlands and subject to EU law and regulations. All data uploaded will reside on servers hosted by SaaSForce which are located in the EU, and cannot be accessed by any organisation other organisation than the host. This means no 3rd party access is allowed, including any Kaspersky Lab entity, unless access is granted explicitly by the customer (e.g. for support purposes). This means that also Kaspersky Lab Benelux, who offers this solution to their customers, has no access to any data.

Requirements:

The Endpoints have to be managed by Kaspersky Security Center (KSC)

Administration server:

• Kaspersky Security Center 10 SP2 (10.3.407.0) or later

KPSN can be used with the following corporate applications from Kaspersky Lab:

- Kaspersky Endpoint Security 10 for Windows SP1 MR2 (10.2.4.674) or later
- Kaspersky Security 10 for Windows Server (10.0.0.486) or later
- Kaspersky Endpoint Security 10 for Mac (10.1.0.622) or later
- Kaspersky Endpoint Security 10 for Linux (10.0.0.3458) or later
- Kaspersky Security for Virtualization 4.0 Agentless (4.0.0.84) or later
- Kaspersky Security for Virtualization 4.0 Light Agent (4.0.46.8060) or later

Configuration steps:

You will get an email with your certificate file. Save the file on a safe place so you can use it for the next operation. In your KSC go to Administration Server and click on Server properties on the right.

Kaspersky Security Center 10 Administration Server KSC108 Managed devices	Administration S	erver KSC10B	(KSC10B\Admi	nistrator)		
Mobile Device Management Device selections	Monitoring	Statistics	Reports	Events		Server properties
Policies						
Tasks Karpersky Lab Licenser	▼ Deployme	▼ Deployment			 Management scheme 	
Advanced	Managed device(s):	Managed device(s): 16. Security application installed on: 15 device(s)			Managed device(s): 16. Unassigned device(s) detected: 0	
	Enable prote	Enable protection			View structure of managed devices	
	Manage Kasp	Manage Kaspersky Security for Virtualization 5.0 Light Agent			Set up automatic moving of devices to groups	
	Protection de	ployment report	IONS		View Unassured devices	

On the right panel, you tick the box: Configure Private KSN. Also, check if the box I agree to use Kaspersky Security Network is ticked. Click on the Select file with KSN settings.

•		Properties: Administration Server KSC10	_ D X
Sections		KSN proxy server settings	
General	^	■ [•] Editing allowed	v () -
Event configuration			
Keys		Use Administration Server as proxy server	
KSN proxy server		☑ I agree to use Kaspersky Security Network	
KSN proxy server settings		✓ Configure Private KSN Select file	with KSN settings
KSN proxy server statistics			
Server connection settings			
Virus outbreak	=		
Traffic			
Events storage		Connection settings:	v 🚺 🗆
Web server		TCP port:	
Revision history storage			
Application categories			
Security			
User roles		C Editing allowed	
Update agents		- Editing anowed	
Tagging rules		Connect slave Administration Servers to KSN through master Administration Server	
Notification delivery settings	~		
<u>Help</u>		ОК Са	ncel Apply

Kaspersky Private Security Network • SaaSForce • Configuration Guide | 3

Select the certificate file that you have saved in the previous step. The file should be a .pkcs7 file.

ĸ	Open		x
⊕ ⊕ - ↑	Desktop 🕨	✓ C Search Desktop	>
Organize 🔻 New	folder	₩ - - (0
Favorites Desktop Downloads	yourcertificate.pkcs7 PKCS7 File 21,3 KB Libraries V	¢	< >
	File name: yourcertificate.pkcs7	All Files (*.*) Open Cancel	- -

You will get a KPSN Statement pop-up with the KPSN EULA.

	KSN Statement	-		x
KPSN EULA	KSN Statement	-		×
	I accept the terms of the KSN Statement		Car	v

Click I accept the terms of the KSN Statement.

Kaspersky Private Security Network • SaaSForce • Configuration Guide | 4

The certificate has been added.

•	Properties: Administration Server KSC10
Sections	KSN proxy server settings
General Event configuration Keys KSN proxy server KSN proxy server settings KSN proxy server statistics Server connection settings Virus outbreak	Editing allowed G Editing allowed G
Traffic Events storage Web server Revision history storage Application categories Security	Connection settings: Connection settings: TCP port: UDP port UDP port UDP port: 15111
User roles Update agents Tagging rules Notification delivery settings	Editing allowed Connect slave Administration Servers to KSN through master Administration Server
<u>Help</u>	OK Cancel Apply

In case of Slave Administration Servers, tick the corresponding box.

Click Apply and you are connected to the KPSN at SaaSforce instead of Global KSN.

There is no downtime from switching from Global KSN to Private KSN.

In the Kaspersky Endpoint Security for Windows policy, the KSN provider has switched from Global to Private KSN.

Within the KSN Proxy settings also select the Use KSN servers when KSN Proxy is not available box. With this setting clients go directly to KPSN when they are not connected to the corporate network.

E	Properties: Kaspersky Endpoint Security for Windows (11.0.0)
High protection level	All recommended protection components are enabled.
Sections	Kaspersky Security Network
General Event configuration Advanced Threat Protection Kaspersky Security Network Behavior Detection Exploit Prevention Host Intrusion Prevention Remediation Engine Essential Threat Protection Security Controls Data Encryption Endpoint Sensor Local tasks General Settings Policy profiles Revision history	✓ Kaspersky Security Network ● ● Kaspersky Security Network (KSN) is a cloud database that contains information about the reputation of files, web resources, and software. - High threat detection rating - Minimal Taise positive rate - Enhanced performance KSN Statement ✓ Enable extended KSN mode KSN settings ✓ Enable cloud mode for protection components ● Computer status when KSN servers are unavailable When cloud mode is enabled: ✓ KSN Proxy Settings ✓ Use KSN Proxy ✓ Use KSN Proxy
Help	OK Cancel Apply

Kaspersky Private Security Network • SaaSForce • Configuration Guide

For Kaspersky Endpoint Security 10 for Mac, Kaspersky Endpoint Security 10 for Linux, Kaspersky Security for Virtualization 4.0 Agentless and Kaspersky Security for Virtualization 4.0 Light Agent no extra steps are needed when the default policy setting are applied.

For the Kaspersky Security 10 for Windows Server an extra step in needed. Within the Kaspersky Security 10 for Windows Server policy, you need to accept the KPSN EULA.

Click on the Data processing button.

	operties: Kaspersky Security 10.1 for Windows Server				
Sections	Real-time server protection				
General Event configuration Application settings Supplementary Real-time server protection Local activity control Network attached storage protection Network activity control System inspection Logs and notifications Revision history	Real-Time File Protection Configure file threat protection settings KSN Usage Configure Kaspersky Security Network usage and read KSN Statement Data processing Settings Traffic Security • Configure web and mail threat protection settings • Configure web control rules Rules list Settings Exploit Prevention • Configure memory protection settings and set exploit prevention techniques Script Monitoring • Configure actions on probably dangerous scripts				
<u>Help</u>	OK Cancel Apply				

And Accept the terms of the KPSN statement and click on OK.

KSN Data processing	? X
Kaspersky Private Security Network	
Please thoroughly read the conditions of the Kaspersky Private Security Network Statement.	
KPSN BLLA	Ā
Accept the terms of the Kaspersky Private Security Network Statement	>
ОК	Cancel

Kaspersky Private Security Network • SaaSForce • Configuration Guide | 6

After that, check KSN Settings.

Check if Use Kaspersky Security Center as KSN proxy box is ticked.

Prop	perties: Kaspersky Security 10.1 for Windows Server					
Sections	Real-time server protection					
General Event configuration Application settings Supplementary Real-time server protection Local activity control Network attached storage protection Network activity control System inspection Logs and notifications Revision history	Real-Time File Protection Configure file threat protection settings KSN Usage Configure Kaspersky Security Network usage and read KSN Statement Data processing Traffic Security • Configure web and mail threat protection settings • Configure web and mail threat protection settings • Configure web control rules Rules list Settings Exploit Prevention Configure memory protection settings and set exploit prevention techniques Script Monitoring Configure actions on probably dangerous scripts					
Help	OK Cancel Apply					

Click on OK.

K	KSN Usage	? X
General	Task management	
Action R L	n to perform on KSN untrusted objects emove og information	
Data ☑ S	transfer 10 not calculate checksum before sending to KSN if file 12 exceeds (MB):	2 ~
KSN F	Proxy Ise Kaspersky Security Center as KSN Proxy	
	ОК	Cancel

Kaspersky Private Security Network • SaaSForce • Configuration Guide

VERIFY KPSN Connection

The following check can be done to see if everything is working properly. Via the properties of KSC:

Click on KSN proxy server statistics and then on Check KSN connection. Connected to KSN means that the connection to the KPSN was successful.

	Properties: Administration Server KSC10				
Sections	KSN proxy server statistics				
General ^ Event configuration	Export to file Refresh				
Keys KSN proxy server KSN proxy server settings KSN proxy server statistics Server connection settings Virus outbreak Traffic Events storage Web server	KSN proxy server activity Cache records: 0 Packages processed in cache: 0 Received packages: 1 Kaspersky Security Center 10 Connected to KSN				
Revision history storage Application categories Security User roles Update agents Tagging rules Notification delivery settings	OK Check KSN connection				
Help	OK Cancel Apply				

Via the Kaspersky Endpoint Security for Windows task, you can check if KSN is available for the clients

Devices	Policies	Tasks					
Create a task	Import task	from file	Add/Ren	move columns			
Inhorited tacks:	hida L show		-			Task "Checking c	connection with KSN" results
Name				Refresh	Use the Refresh button	to display the latest results of the t	ask.
Checking con	nection with KSN		5	ime	Device *	Status	Description
Find vulnerab	ilities and required	d updates	G	11-7-2018 16:09:32	VDI-03	Completed	KSN servers available
📋 Install required	d updates and fix	vulnerabilities	Ĩ	11-7-2018 16:09:31	VDI-05	Completed	KSN servers available
📋 Quick Virus Sc	an						
🔲 Update							
📋 Virus scan							

KASPERSKY®

Support

Kaspersky Lab

Kaspersky Lab customers can log a case via https://companyaccount.kaspersky.com/ Kaspersky Lab resellers can call the Kaspersky Lab partner support for assistance Kaspersky Lab partner support phone: +31 307529529

SaaSForce

SaaSForce will deliver first line support to Kaspersky Lab resellers only. Kaspersky Lab customers can contact their Kaspersky Lab reseller for assistance. SaaSForce will support, manage and maintain this hosted environment. During business hours EU CET time, you can reach SaaSForce by phone +32 38778293 or by email at: KPSN@saasforce.eu



© 1997 – 2018 Kaspersky Lab. All Rights Reserved.



The Cloud Services Provider