KASPERSKY lab

Kaspersky Threat Intelligence Portal for QRadar

Product version: 1.0

Dear User,

Thank you for choosing Kaspersky Lab as your security software provider. We hope that this document helps you to use our product.

Document revision date: 28.03.2018

https://www.kaspersky.com
https://help.kaspersky.com
https://support.kaspersky.com

Contents

About this document

This document describes Kaspersky Threat Intelligence Portal for QRadar.

About Kaspersky Threat Intelligence Portal for QRadar

Kaspersky Threat Intelligence Portal for QRadar is an app for IBM® QRadar®.

Kaspersky Threat Intelligence Portal for QRadar provides the following functionality:

- Quick and easy access to threat intelligence (TI) from Kaspersky Threat Intelligence Portal about indicators in events stored in QRadar.
- Creation of links for indicators that allow searching for the indicators in Kaspersky Threat Intelligence Portal.
- Access to Kaspersky Threat Intelligence Portal for full Kaspersky Lab information about cyber-threats, legitimate objects, and their relationships.
- Enriched indicators provide the user with full context in just two clicks of the mouse.

Software requirements

Kaspersky Threat Intelligence Portal for QRadar has the following software requirements:

- QRadar 7.2.8 or later

About Kaspersky Threat Intelligence Portal

Kaspersky Threat Intelligence Portal for QRadar interoperates with Kaspersky Threat Intelligence Portal. Kaspersky Threat Intelligence Portal provides reliable, immediate intelligence about cyber-threats, legitimate objects, and their inter-connections and indicators. This intelligence is enriched with actionable context to inform your business or clients about associated risks and implications. This allows you to mitigate and respond to threats more effectively, defending against attacks even before they are launched.

Kaspersky Threat Intelligence Portal delivers all the knowledge acquired by Kaspersky Lab about cyber-threats and their relationships, brought together into a single, powerful web service. The goal is to provide your security teams with as much data as possible, preventing cyber-attacks before they impact your organization. The platform retrieves the latest detailed threat intelligence about URLs, domains, IP addresses, file hashes: the threat names, statistical or behavior data, WHOIS or DNS data, and other data. The result is global visibility of new and emerging threats, which helps you secure your organization and boosts incident response.

To get access to Kaspersky Threat Intelligence Portal, you need a certificate (see Section "About Kaspersky Lab certificate" on page 13). You can request a certificate for Kaspersky Threat Intelligence Portal by filling in the request form at http://www.kaspersky.com/enterprise-security/intelligence-services.

If you have any technical issues related to the work of Kaspersky Threat Intelligence Portal for QRadar, please contact us at intelligence@kaspersky.com. Email support is provided during weekday business hours (Russia, UTC/GMT +3).

Kaspersky Threat Intelligence Portal for QRadar

This section describes how to install, use, and uninstall Kaspersky Threat Intelligence Portal for QRadar.

In this chapter

Installing Kaspersky Threat Intelligence Portal for QRadar

This section describes how to install Kaspersky Threat Intelligence Portal for QRadar.

► *To install Kaspersky Threat Intelligence Portal for QRadar:*

1. In QRadar, select **Admin** and then **Extensions Management**.
2. In the **Extensions Management** form, click the **Add** button.
3. Select the application file archive.
4. Select the **Install immediately** check box.
5. Click **Add**.
6. Click **Install**.
7. Click **Install** again.

Kaspersky Threat Intelligence Portal for QRadar appears in the **Extensions Management** form after it is installed.

8. Refresh the browser window before you use the app.

After Kaspersky Threat Intelligence Portal for QRadar is installed, the **Log Activity** page will contain a new **Lookup in Kaspersky TI** button..

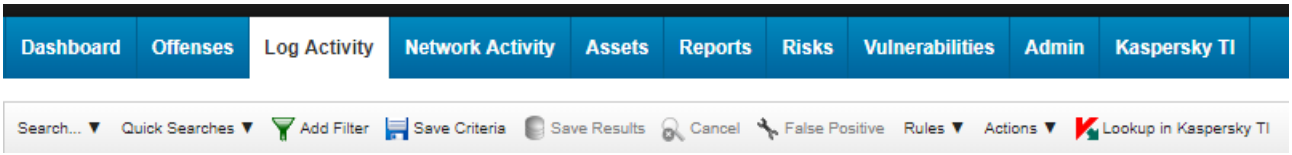

Figure 1. Lookup in Kaspersky TI button

Using Kaspersky Threat Intelligence Portal for QRadar

This section describes how to use Kaspersky Threat Intelligence Portal for QRadar.

► *To use Kaspersky Threat Intelligence Portal for QRadar:*

1. On the **Log Activity** tab, select one or several rows of the table.
2. Click the **Lookup in Kaspersky TI** button.

   Kaspersky Threat Intelligence Portal for QRadar finds indicators in the selected table rows and opens a window that displays unique indicators with hyperlinks.
3. Click a hyperlink to open a Kaspersky Threat Intelligence Portal window with the threat intelligence about the selected indicator.

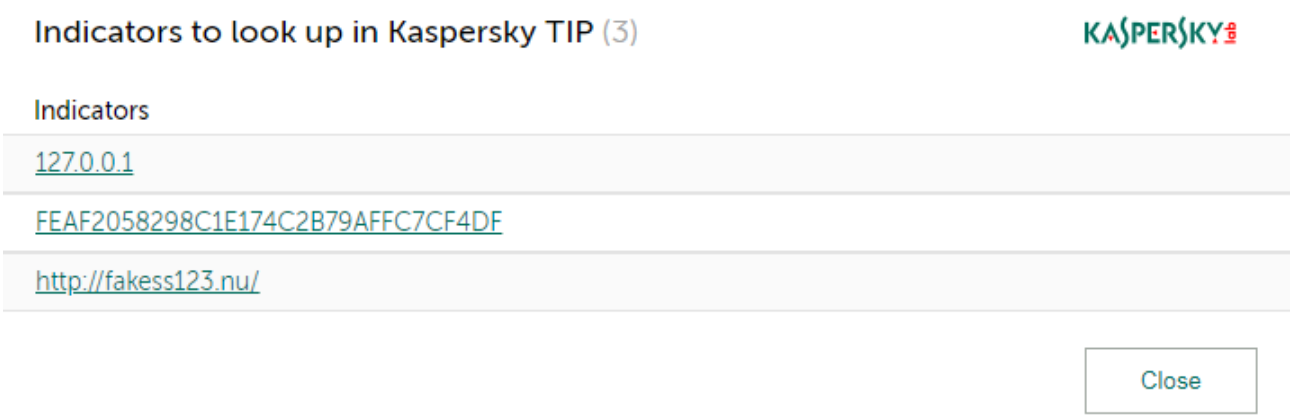

Figure 2. Indicators to look up in Kaspersky TIP

Indicators of the following types are extracted:

- IPv4 addresses
- Hashes (MD5, SHA1, SHA256)
- URLs

Kaspersky Threat Intelligence Portal for QRadar extracts only those indicators that are present in the table. If an event contains indicators that are not displayed in visible fields, these indicators will not be extracted. To add such indicators to the extracted ones, make the fields that contain these indicators visible by clicking **Search** > **Edit Search**.

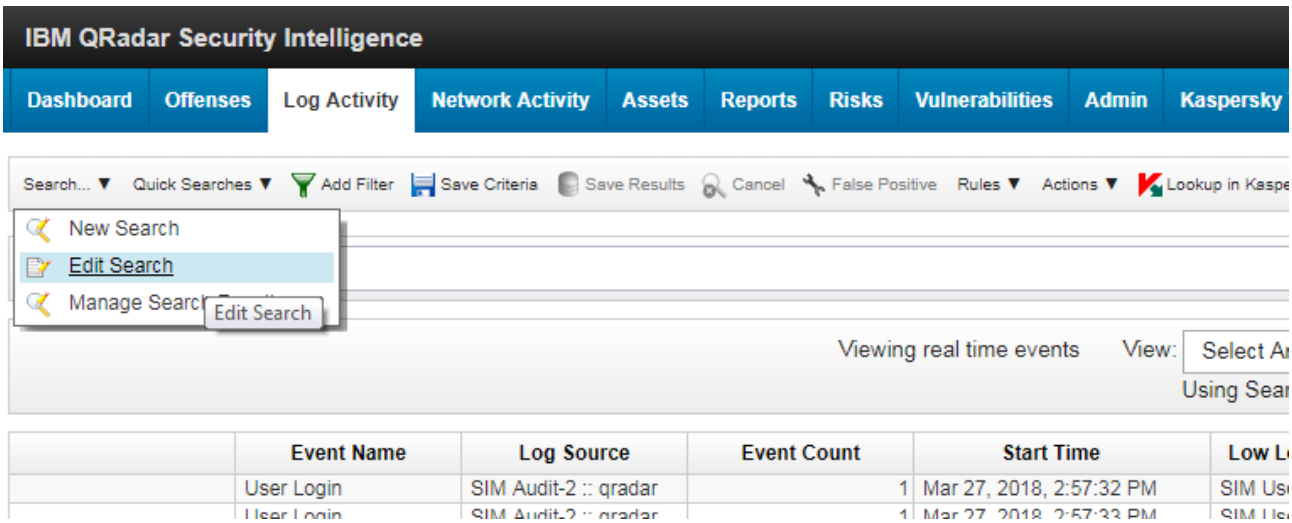

Figure 3. Configuring search table

You can also right-click an IP address contained in a cell of the table on the **Log Activity** page. The context menu of the table cell will contain a **Lookup in Kaspersky TI** item (or a **More Options | Lookup in Kaspersky TI** item). If you select this item, a Kaspersky Threat Intelligence Portal window opens with the threat intelligence about the IP address.

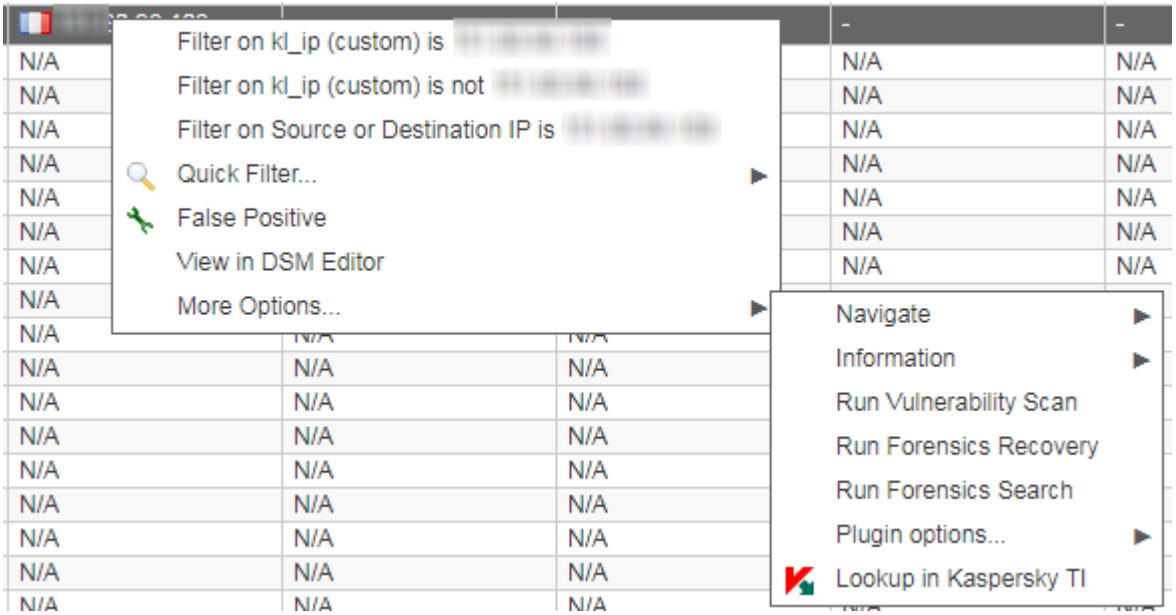

Figure 4. More Options | Lookup in Kaspersky TI menu item

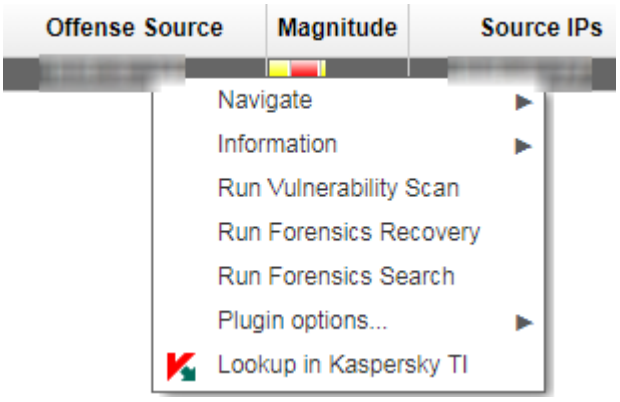

Figure 5. Lookup in Kaspersky TI menu item

Uninstalling Kaspersky Threat Intelligence Portal for QRadar

This section describes how to uninstall Kaspersky Threat Intelligence Portal for QRadar.

► *To uninstall Kaspersky Threat Feed Service App:*

1. In QRadar Console, select **Admin** > **Extensions Management**.
2. In the **Extensions Management** form, select the **INSTALLED** tab.
3. Select the `Kaspersky Threat Intelligence Portal for QRadar` item and click **Uninstall**.

After Kaspersky Threat Intelligence Portal for QRadar is uninstalled, the **Lookup in Kaspersky TI** tab disappears from QRadar Console.

About Kaspersky Lab certificate

You can gain access to Kaspersky Threat Intelligence Portal if you imported the Kaspersky Lab certificate to the Microsoft® Windows® certificate storage. The certificate is provided after you purchase a license from Kaspersky Lab.

In Windows, you can import the certificate to the certificate storage by using the Certificate Import Wizard. To run the Wizard, double-click the certificate. When using the Wizard, select the relevant check box to mark the private key as exportable, as shown in the figure below.

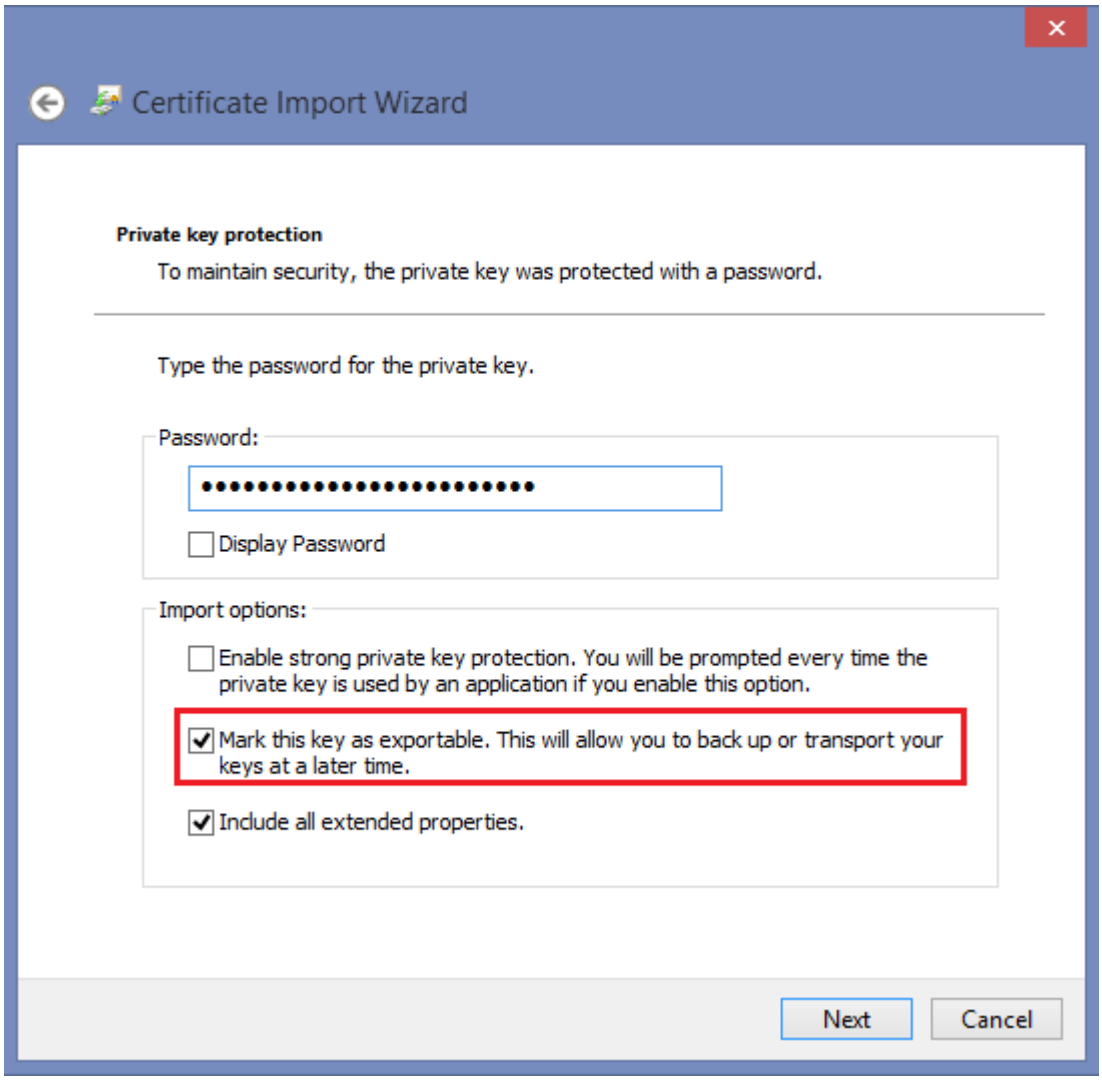

Figure 6. Certificate Import Wizard

If the browser that you use to gain access to QRadar Console does not use the system certificate storage (for example, if it is the Mozilla™ Firefox™ browser), import the Kaspersky Lab certificate to the certificate storage of this browser.

In Linux®, you must use a PEM-formatted certificate. If the delivered certificate is in PFX format, convert it to PEM format. To do this, it is recommended that you use OpenSSL.

One of the ways to use OpenSSL to convert a certificate to PEM format is to run the following command.

```
openssl pkcs12 -in <certificate_name>.pfx -clcerts -out
<certificate_name>.pem -nodes
```

AO Kaspersky Lab

Kaspersky Lab is a world-renowned vendor of systems protecting computers against digital threats, including viruses and other malware, unsolicited email (spam), and network and hacking attacks.

In 2008, Kaspersky Lab was rated among the world's top four leading vendors of information security software solutions for end users (IDC Worldwide Endpoint Security Revenue by Vendor). Kaspersky Lab is the preferred vendor of computer protection systems for home users in Russia (IDC Endpoint Tracker 2014).

Kaspersky Lab was founded in Russia in 1997. It has since grown into an international group of companies with 38 offices in 33 countries. The company employs more than 3,000 skilled professionals.

Products. Kaspersky Lab products provide protection for all systems, from home computers to large corporate networks.

The personal product range includes security applications for desktop, laptop, and tablet computers, smartphones and other mobile devices.

The company offers protection and control solutions and technologies for workstations and mobile devices, virtual machines, file and web servers, mail gateways, and firewalls. The company's portfolio also features specialized products providing protection against DDoS attacks, protection for industrial control systems, and prevention of financial fraud. Used in conjunction with centralized management tools, these solutions ensure effective automated protection for companies and organizations of any size against computer threats. Kaspersky Lab products are certified by major test laboratories, compatible with software from diverse vendors, and optimized to run on many hardware platforms.

Kaspersky Lab virus analysts work around the clock. Every day they uncover hundreds of thousands of new computer threats, create tools to detect and disinfect them, and include their signatures in databases used by Kaspersky Lab applications.

Technologies. Many technologies that are now part and parcel of modern anti-virus tools were originally developed by Kaspersky Lab. It is no coincidence that many other developers use the

Kaspersky Anti-Virus engine in their products, including: Alcatel-Lucent, Alt-N, Asus, BAE Systems, Blue Coat, Check Point, Cisco Meraki, Clearswift, D-Link, Facebook, General Dynamics, H3C, Juniper Networks, Lenovo, Microsoft, NETGEAR, Openwave Messaging, Parallels, Qualcomm, Samsung, Stormshield, Toshiba, Trustwave, Vertu, and ZyXEL. Many of the company's innovative technologies are patented.

Achievements. Over the years, Kaspersky Lab has won hundreds of awards for its services in combating computer threats. Following tests and research conducted by the reputed Austrian test laboratory AV-Comparatives in 2014, Kaspersky Lab ranked among the top two vendors by the number of Advanced+ certificates earned and was ultimately awarded the Top Rated certificate. But Kaspersky Lab's main achievement is the loyalty of its users worldwide. The company's products and technologies protect more than 400 million users, and its corporate clients number more than 270,000.

Kaspersky Lab website:	https://www.kaspersky.com
Virus encyclopedia:	https://securelist.com
Virus Lab:	https://virusdesk.kaspersky.com (for analyzing suspicious files and websites)
Kaspersky Lab's web forum:	https://forum.kaspersky.com

Trademark notices