

QRadar Support Forums

Jonathan Pechta
Support Content Lead

Kim McCall
Social Engagement Manager

<https://ibm.biz/qradarforums>

Agenda

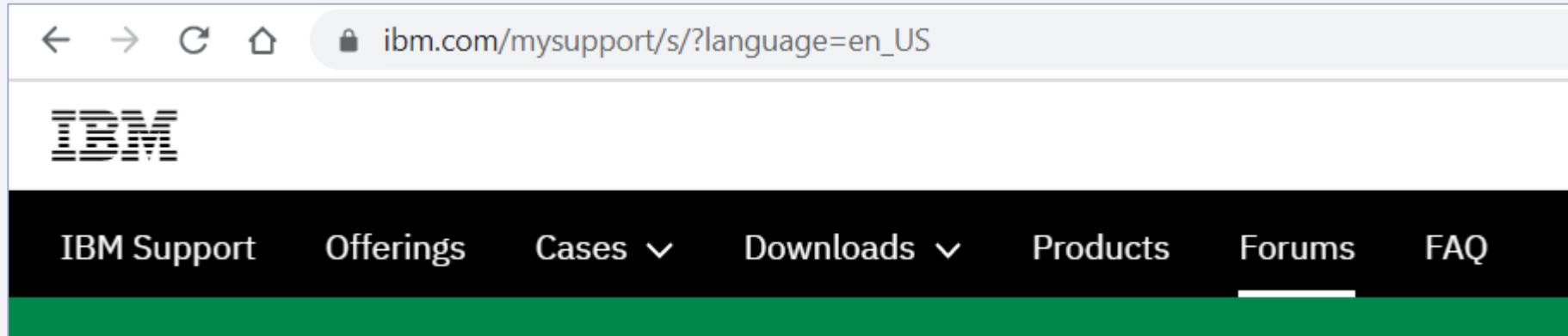
Announcements	03
About the forum migration	04
Navigating the forum user interface	05
Product forums	06
Using forum tags	07
Asking questions and getting support help	09
Answering questions	10
Staying up-to-date	11
Site assistance and feedback	12

Announcements

- Coming soon, new firmware releases:
 - M6 appliance firmware v1.0.0
 - M5 appliance firmware v5.0.0
- QRadar 7.4 is released. A list of features is posted on the QRadar 101 main page.
- A QRadar 7.4 compatible SFS file WinCollect 7.2.9 Patch 1 has been posted to IBM Fix Central.
- Google Cloud users might be interested in the new Google Cloud Pub/Sub integration release.

About the forum migration

The IBM Developerworks Answers forum is being migrated to IBM.com/mysupport on 1 April 2020.



Why?

- Better integration with support cases.
- All IBM products in one forum together.
- Unify the support experience for users.

Navigating the forum user interface

The screenshot shows the IBM Support forum homepage. A red arrow labeled '1' points to the 'Support Forums' heading. A red arrow labeled '2' points to the 'Recently used tags' section. A red arrow labeled '3' points to the 'My questions (0)' and 'My replies (0)' buttons. A red arrow labeled '4' points to the post statistics (3 answers, 2 likes, 442 views) for a specific thread. A red arrow labeled '5' points to the 'Ask a question' button.

IBM

Marketplace

IBM Support Offerings Cases Downloads Products Forums FAQ

Search support

Open a case

Support Forums

Search forums

Ask a question

Most popular Newest Most liked

20

My products

Select or search for a product

Recently used tags

Maximo Asset Management

Cognos Analytics (formerly Cognos Business Inte...)

MAC OS Mojave HCL Notes Client

QRadar SIEM Planning Analytics Local

Db2 Linux, Unix and Windows

My questions (0) My replies (0)

updated 8 days ago

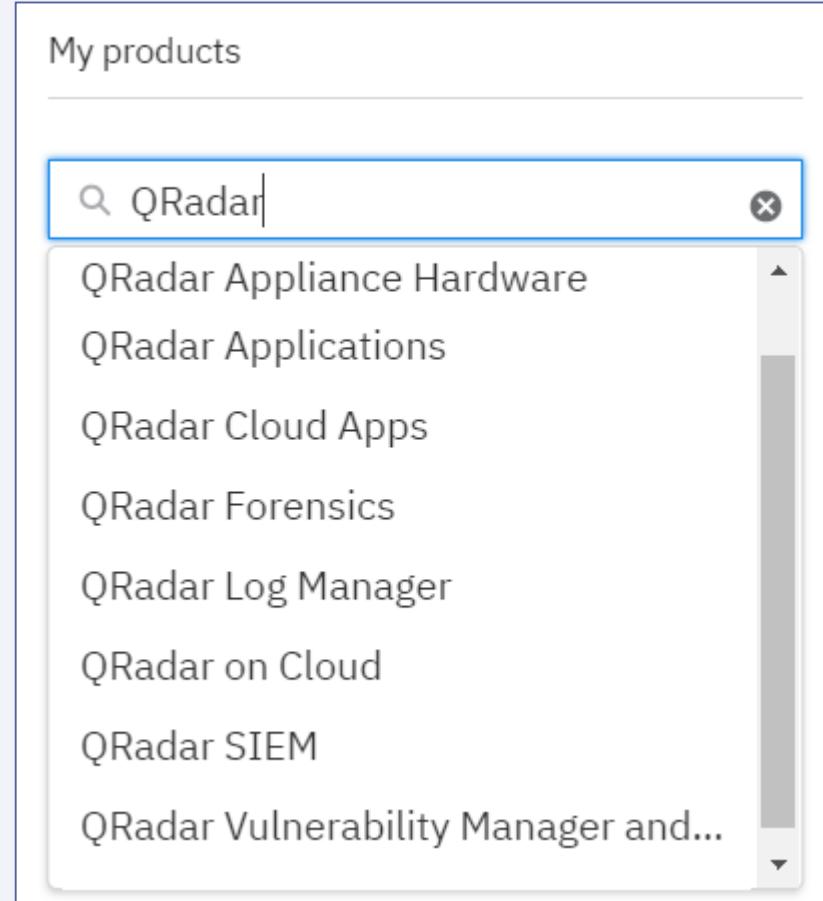
1 2 3 4 5

Product forums

Each product in the IBM forums has a forum area.

What to know

- Each question asked in the forums is sorted under a product.
- Questions must include a product tag, then extra topic tags can be added.
- It is easiest to type SIEM to filter for QRadar from the product list.
- Updates to the product list are still pending, for example, to add QRadar Network Insights.



The screenshot shows a search interface with a search bar at the top containing the text "QRadar". Below the search bar is a list of product names. The products listed are: QRadar Appliance Hardware, QRadar Applications, QRadar Cloud Apps, QRadar Forensics, QRadar Log Manager, QRadar on Cloud, QRadar SIEM, and QRadar Vulnerability Manager and... The list is scrollable, indicated by a vertical scrollbar on the right side of the interface.

My products

QRadar

QRadar Appliance Hardware

QRadar Applications

QRadar Cloud Apps

QRadar Forensics

QRadar Log Manager

QRadar on Cloud

QRadar SIEM

QRadar Vulnerability Manager and...

Using forum tags

What to know

- Users can create their own tags.
- A maximum of 10 tags per question, including the automatic product tag (i.e. **9** topic tags can be added).
- An individual tags cannot exceed **60** characters.
- Tags are not case-sensitive. The system converts every tag to lowercase to prevents duplicate tags.
- To create multiple-word tags, use hyphens between words (ex. system-fan-noise). The Forums converts underscore characters to hyphens, and ignores leading or trailing underscores and hyphens.
- When three characters are typed in the tag field, the system displays a search list for existing tags containing those characters.

The screenshot shows a web-based support forum interface. At the top, there is a search bar with the text 'API' and a blue 'Ask a question' button. Below the search bar, the page title is 'Support Forums' with a 'Back to forums home' link. The main content area is titled 'QRadar SIEM' and has a 'Recent questions' tab selected. A list of search results is displayed, including:

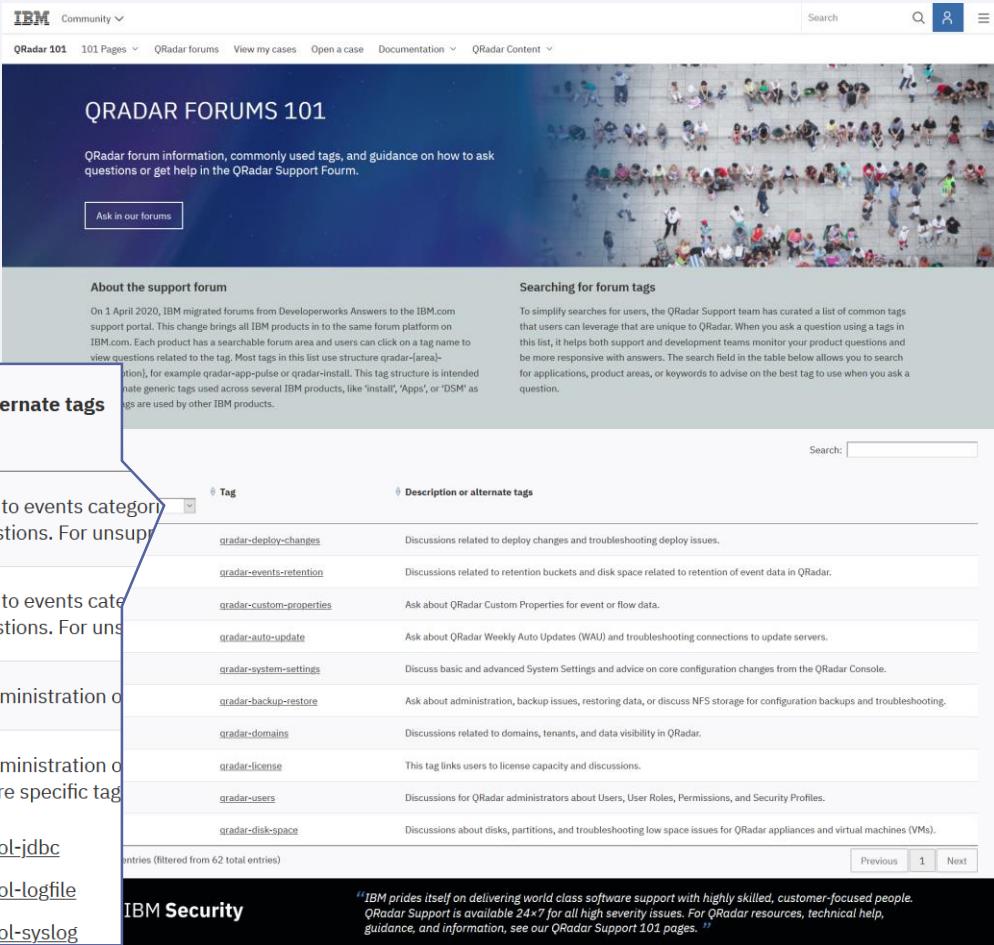
- Securing the API(masking property variables) in API...
- API Connect on premise - manage secure external api
- TLS mutual authentication in apiConnect for individ...
- Sample API
- Rhapsody API
- API is not reliable
- FTP api
- API BreakHere

On the right side of the search results, there is a sidebar with a dropdown menu set to '20', a question 'How to secure API traffic in QRadar SIEM?', and a post from 'david.joshua' with 1 answer, 0 likes, and 104 views. The post title is 'Best Practices for collecting Database audit logs in QRADAR' and it was asked by 'v.saykov' on '19 Jun 2019'. The sidebar also shows a message about encrypted tunnels and a note that the post was updated 6 months ago.

Forum tags (continued)

Taking the guess work out of tags...

- Starting April 1, a master tag list is being maintained by the QRadar Support Team.



The screenshot shows the QRadar Support Forum homepage. At the top, there is a navigation bar with links for 'QRadar 101', '101 Pages', 'QRadar forums', 'View my cases', 'Open a case', 'Documentation', and 'QRadar Content'. The main title 'QRADAR FORUMS 101' is displayed, along with a sub-header: 'QRadar forum information, commonly used tags, and guidance on how to ask questions or get help in the QRadar Support Forum.' A 'Ask in our forums' button is present. Below this, there are two sections: 'About the support forum' and 'Searching for forum tags'. The 'About the support forum' section contains text about the migration of forums from Developerworks Answers to the IBM.com support portal. The 'Searching for forum tags' section lists a curated list of common tags. A blue line from the 'Category' dropdown in the table below points to the 'gradar-events-unknown' tag in the list. A blue box highlights the 'gradar-events-unknown' tag and its description in the table below.

Category	Tag	Description or alternate tags
Events and Log Sources	gradar-events-unknown	Questions related to events category and QID map questions. For unsupported events.
Events and Log Sources	gradar-events-stored	Questions related to events category and QID map questions. For unsupported events.
Events and Log Sources	gradar-dsm-editor	Use this tag for administration of QRadar DSMs.
Events and Log Sources	gradar-protocols	Use this tag for administration of QRadar protocols. For more specific tags: <ul style="list-style-type: none">gradar-protocol-jdbcgradar-protocol-logfilegradar-protocol-syslog

Functionality overview (Demo)

Ask questions in the Q&A panel

Asking questions and getting support help

What to know

- Use QRadar Forums 101 to identify tags being monitored by QRadar Support and Development teams.
- Using the Space, Enter, or Comma keys will end the tag search.
- You can always identify unique qradar tags as they will use the format **qradar-{area}-{topic}**.
- Tags that do not start with qradar- might apply to any IBM product.
- If you are having issues and not sure where to turn, use the tag **qradar-help**.

Ask a question

*Product

QRadar SIEM

*Question

How do I.....

How do I configure multiple event retention buckets with tenants in my domain?

Tags

domain

Domains

domainadministratornotfoundexception

domainuser

domainid

#domain

cross-domain

Answering questions

What to know

- Accepted 'best' answers are marked in Green blocks.
- Questions with answers list the number of responses, but only 'accepted' answers
- It is easiest to type SIEM to filter for QRadar from the product list.
- Updates to the product list are still pending, for example, to add QRadar Network Insights.

1 answers

0 likes

1 views

Cutom email notification template
asked by [REDACTED] 21 Jun 2019

I am following the instruction from https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.1/com.ibm.qradar.doc/t_CONFIGURING_CUSTOM_EMAIL_NOTIFICATIONS.html to create new email notification template.

When I create a new rule, I can select the new template name. However for some reason, the body of the e-mail still using the old default e-mail template. Any reason why?

Also is there any documentation explaining on how to add more than 18 lines of parameters?

Thanks a lot for your help.

qradarce Email Notification QRadar SIEM updated 6 days ago | [REDACTED]

4 answers

QRadar 7.3.1 Patch 8, TLS syslog protocol is missing
asked by [REDACTED] 19 Jun 2019

[REDACTED] (1)

13 Feb 2020 (2 months ago)

Hi, The QRadar CE- edition does permit usage for SOC analyst for testing purposes. Especially, if your production environment is in 7.3.3.x. Regards, Sree

Likes - 1

Like Reply **Select as Accepted answer**

Staying up-to-date

- QRadar Assistant App v3.0 includes a feed for the 'QRadar SIEM' product tag from the IBM.com/mysupport forums.
- The forum feed integration links users to the latest questions asks. Clicking an answer or question takes users to the ibm.com/mysupport forum
- We are investigating how to also add this feed to the Forums 101 page.

Support Forum

The latest QRadar related questions from IBM forums

How to edit QRadar's default email template?

Hello: We want to edit QRadar's offense notification rule, in which an email is sent to a chosen address with a default offense template. The default template's offense shows the following title: "Offense CRE Rule #XXXXXX, Ticketing Offenses fired.". We would like to edit it to show the title of the offense it is reporting. Thanks in advance.

[View 1 answer](#)

How to purge Add data from QRadar?

Trouble with RegEx in Qradar.

Cannot display Qradar Log sources list

Where did the network Hierarchy files go?

QRadar McAfee Advanced Threat Defense (ATD) DSM

Site assistance and feedback

If you have access issues, login problems, or general site trouble you can report an issue to IBM.

Each page has a Report link in the footer that can be used when you cannot access cases, forums, or other site issues.

[Report a problem submitting a case or registering for support.](#)



Tip: If you have QRadar specific forum feedback, questions, or have tag suggestions, use the tag:
qradar-forum-feedback

(optional: jonathan.pechta1@ibm.com)

Get help - report an issue with this website X

[Chat with help desk](#)

*If you have a question or problem with a product, please open a case

* Select a topic

Select a topic

Adding and removing users
Error: not authorized
Need access to cases
Problem opening a case
Received an error message
Site usage question
Suggestion or feedback
Other issue or question
Support access question

* Provide your email address so we can reply.

Submit

Questions?

Ask questions in the Q&A panel

Thank you

Follow us on:

ibm.com/security

securityintelligence.com

ibm.com/security/community

xforce.ibmcloud.com

[@ibmsecurity](https://twitter.com/ibmsecurity)

[youtube/user/ibmsecuritysolutions](https://www.youtube.com/user/ibmsecuritysolutions)

© Copyright IBM Corporation 2019. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

