

QRadar Support Forums

Jonathan Pechta
Support Content Lead

Kim McCall
Social Engagement Manager

<https://ibm.biz/qradarforums>

Agenda

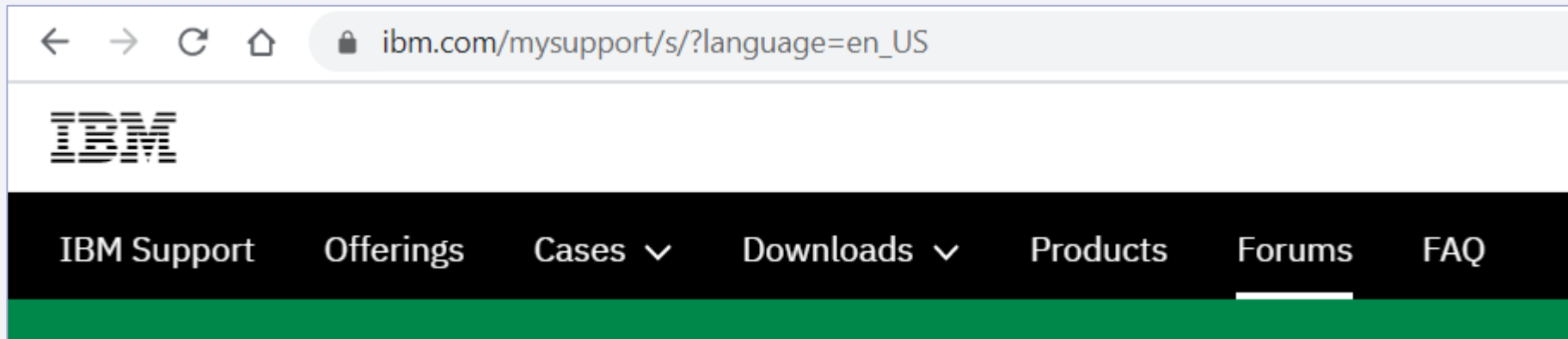
Announcements	03
About the forum migration	04
Navigating the forum user interface	05
Product forums	06
Using forum tags	07
Asking questions and getting support help	09
Answering questions	10
Staying up-to-date	11
Site assistance and feedback	12

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 displays the IBM Support Forums interface. At the top, the IBM logo is on the left, and a 'Marketplace' button and a user profile icon are on the right. Below this is a dark navigation bar containing links for 'IBM Support', 'Offerings', 'Cases', 'Downloads', 'Products', 'Forums' (which is highlighted), and 'FAQ'. A search bar labeled 'Search support' and an 'Open a case' button are also present in this bar.

The main content area is titled 'Support Forums'. It features a 'Search forums' input field (annotated with a red arrow and the number 1) and a blue 'Ask a question' button (annotated with a red arrow and the number 5). Below the search field are three tabs: 'Most popular' (selected), 'Newest', and 'Most liked'. To the right of these tabs is a dropdown menu showing '20' items.

The first forum post is titled 'Performance of Notes Client Release 10.0.1 gets slow after mi...' and was asked by a user on 11 Nov 2019. To the left of the post title, the statistics are shown: 3 answers, 2 likes, and 442 views (annotated with a red arrow and the number 4). The post content describes a performance issue after migrating from Sierra to Catalina on an iMac. It asks for advice on configuration adjustments to improve performance. The post is signed 'Tks in advance,' and includes a redacted signature.

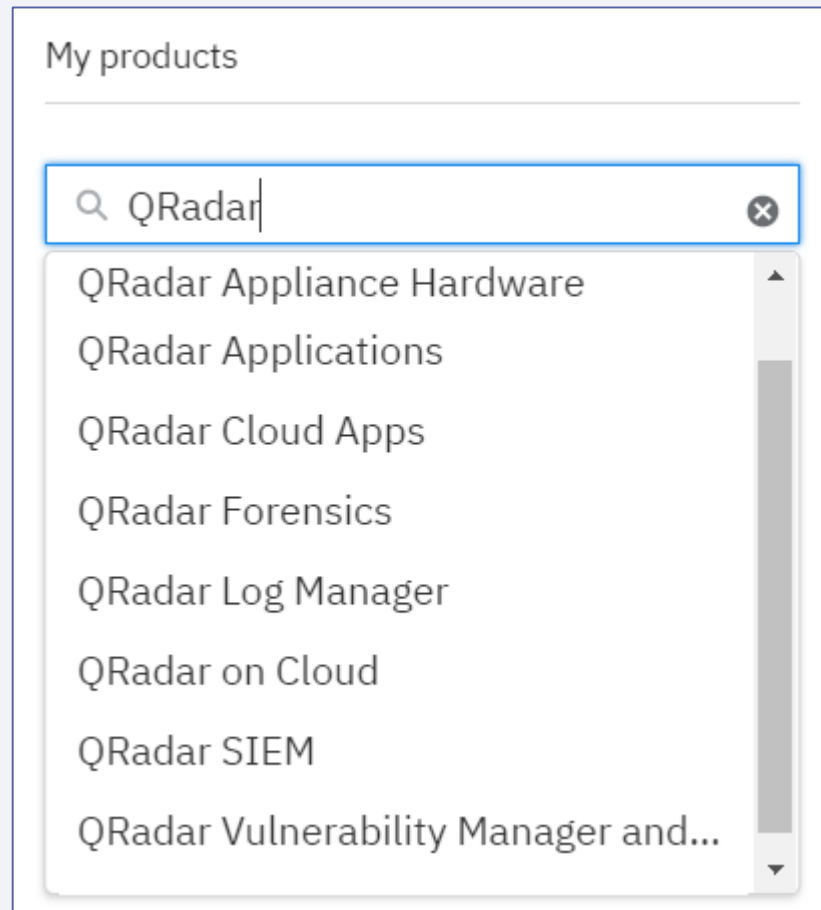
On the right side of the forum, there are two sections: 'My products' and 'Recently used tags'. The 'My products' section has a search bar labeled 'Select or search for a product' (annotated with a red arrow and the number 2). The 'Recently used tags' section lists several tags: 'Maximo Asset Management', 'Cognos Analytics (formerly Cognos Business Inte...', 'MAC OS Mojave', 'HCL Notes Client', 'QRadar SIEM', 'Planning Analytics Local', and 'Db2 Linux, Unix and Windows' (annotated with a red arrow and the number 3). At the bottom of this section, there are links for 'My questions (0)' and 'My replies (0)'.

Product forums

Each product in the IBM forums has a forum area.

What to know

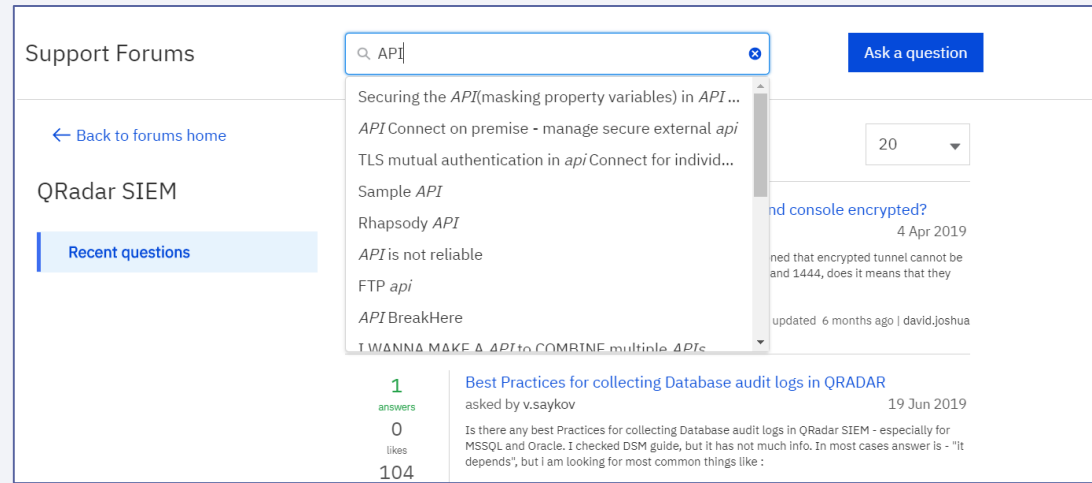
- Each question asked in the forums is sorted under a product.
- Questions must include a product tag, then extra topic tags can be added.
- It is easiest to type SIEM to filter for QRadar from the product list.
- Updates to the product list are still pending, for example, to add QRadar Network Insights.



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.



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 image shows a screenshot of the IBM QRadar Forums 101 page. The page header includes the IBM logo, 'Community', and navigation links like 'QRadar 101', '101 Pages', 'QRadar forums', 'View my cases', 'Open a case', 'Documentation', and 'QRadar Content'. The main heading is 'QRADAR FORUMS 101'. Below it, a subheading reads: 'QRadar forum information, commonly used tags, and guidance on how to ask questions or get help in the QRadar Support Forum.' There is a button that says 'Ask in our forums'. The page is divided into two columns. The left column is titled 'About the support forum' and contains text about the migration of forums from Developerworks Answers to the IBM.com support portal. The right column is titled 'Searching for forum tags' and explains that the QRadar Support team has curated a list of common tags to help users find answers more quickly. Below this, there is a search bar and a table of tags. The table has two columns: 'Tag' and 'Description or alternate tags'. The table lists various tags such as 'qradar-events-unknown', 'qradar-events-retention', 'qradar-custom-properties', 'qradar-auto-update', 'qradar-system-settings', 'qradar-backup-restore', 'qradar-domains', 'qradar-license', 'qradar-users', and 'qradar-disk-space'. A callout box from the text 'Taking the guess work out of tags...' points to the 'qradar-events-unknown' tag in the table. The callout box contains a detailed view of the tag, showing its category ('Events and Log Sources'), its description ('Questions related to events category and QID map questions. For unsupported events, for example qradar-app-pulse or qradar-install. This tag structure is intended to be generic tags used across several IBM products, like 'install', 'App', or 'DSM' as they are used by other IBM products.'), and a list of related tags: 'qradar-protocol-jdbc', 'qradar-protocol-logfile', and 'qradar-protocol-syslog'.

Category	Tag	Description or alternate tags
Events and Log Sources	qradar-events-unknown	Questions related to events category and QID map questions. For unsupported events, for example qradar-app-pulse or qradar-install. This tag structure is intended to be generic tags used across several IBM products, like 'install', 'App', or 'DSM' as they are used by other IBM products.
Events and Log Sources	qradar-events-stored	Questions related to events category and QID map questions. For unsupported events, for example qradar-app-pulse or qradar-install. This tag structure is intended to be generic tags used across several IBM products, like 'install', 'App', or 'DSM' as they are used by other IBM products.
Events and Log Sources	qradar-dsm-editor	Use this tag for administration of the DSM editor in QRadar. For more specific tag questions, see the list of tags below.
Events and Log Sources	qradar-protocols	Use this tag for administration of protocols in QRadar. For more specific tag questions, see the list of tags below.

Tag	Description or alternate tags
qradar-deploy-changes	Discussions related to deploy changes and troubleshooting deploy issues.
qradar-events-retention	Discussions related to retention buckets and disk space related to retention of event data in QRadar.
qradar-custom-properties	Ask about QRadar Custom Properties for event or flow data.
qradar-auto-update	Ask about QRadar Weekly Auto Updates (WAU) and troubleshooting connections to update servers.
qradar-system-settings	Discuss basic and advanced System Settings and advice on core configuration changes from the QRadar Console.
qradar-backup-restore	Ask about administration, backup issues, restoring data, or discuss NFS storage for configuration backups and troubleshooting.
qradar-domains	Discussions related to domains, tenants, and data visibility in QRadar.
qradar-license	This tag links users to license capacity and discussions.
qradar-users	Discussions for QRadar administrators about Users, User Roles, Permissions, and Security Profiles.
qradar-disk-space	Discussions about disks, partitions, and troubleshooting low space issues for QRadar appliances and virtual machines (VMs).

IBM Security

"IBM prides itself on delivering world class software support with highly skilled, customer-focused people. QRadar Support is available 24x7 for all high severity issues. For QRadar resources, technical help, guidance, and information, see our QRadar Support 101 pages."

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**.

The screenshot shows a web form titled "Ask a question". It has three main sections: "Product", "Question", and "Tags".

- Product:** A dropdown menu with a search icon and a close button (X). The selected value is "QRadar SIEM".
- Question:** A text input field containing "How do I.....". Below it is a rich text editor toolbar with buttons for Bold (B), Italic (I), Underline (U), Strikethrough (ABC), Bulleted List, Numbered List, Indent Left, Indent Right, and Link (Tx). The text area below the toolbar contains the question: "How do I configure multiple event retention buckets with tenants in my domain?".
- Tags:** A search input field with a search icon and a close button (X). The text "domain" is entered. Below the input is a scrollable list of suggestions: "Domains", "domainadministratortnotfoundexception", "domainuser", "domainid", "#domain", and "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

Custom 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

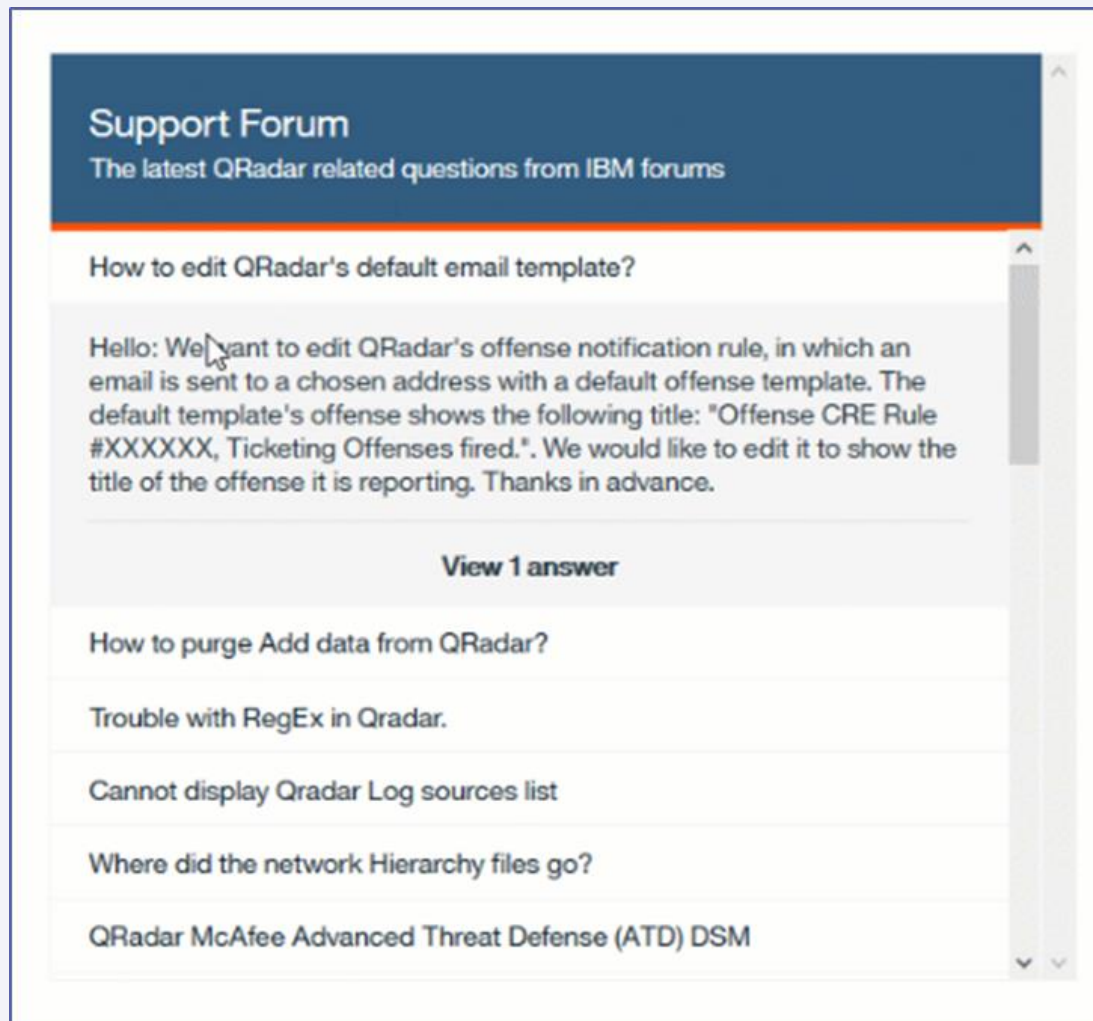
 Like

 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.



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

Chat with help desk

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

* Select a topic

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

© 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.

IBM Security



