Splunk® Answers and Splunkbase Splunk Answers User Manual splunkbase

Generated: 1/22/2020 2:18 am

Copyright (c) 2020 Splunk Inc. All Rights Reserved
Introduction

About Answers

Splunk Answers is a community site where you can ask and answer specific questions relating to Splunk. You can:

- post a question
- answer a question
- comment on a question or answer
- search for information posted by others
- upvote and downvote questions and answers

Splunk community guidelines

Basically, don't be a jerk.

Be nice. Treat others with the same respect you'd want them to give you. We're all here to learn together. Be tolerant of others who might not know everything you know. Bring your sense of humor.

Be honest. Above all, be honest. If you see misinformation, insert comments indicating what, specifically, is wrong. Even better -- edit and improve the information! Provide stronger, faster, superior answers of your own!

Be helpful. If you see a good answer to a question, vote it up. If your question has been answered, please click "Accept" below the answer that best addressed your issue, in order to resolve the post. This community site depends on your participation.

Don't promote your business or spam on Answers.

In addition to these simple rules for behavior on Splunk Answers, users must follow the Community Guidelines that apply to all Splunk Community programs.
Contact us

- If you have Splunk Answers account issues, problems posting content, or have found a bug on the Answers site, send an email with a brief description and screenshots to answers-support@splunk.com and a member from the Splunk Community team will respond as soon as possible.
- If you have a post that is awaiting moderation, it will be reviewed and published once a moderator is available. The delay at night (US time) can be several hours as we are not yet staffed for 24-hour coverage.
- **Do not** contact us for help with Splunk product questions. If you are having trouble getting an answer for a question you posted on Answers, follow these guidelines to increase your chances of getting a response.
Ask and answer questions

You can begin your Splunk Answers community participation by asking or answering a question.

How to ask a question

If you've got a specific question about using, deploying, or troubleshooting a problem with Splunk, you can first search Documentation, then search Splunk Answers to see if a similar question to yours has already been posted.

If no one else has asked your question, navigate to https://answers.splunk.com/answers and click Ask a question, next to the search bar.

The title of your question should be as clear as possible. What exactly are you asking? Do you want help with a field extraction? If so, a title like "Need help writing a field extraction that does <xyz>". Are you seeing an error in your Splunk logs and want help figuring out what it means? "Seeing the following error <error snippet>, what does it mean?" is a clear question title.

In the text of your question, provide as much detailed info about your situation and environment as you can, taking care not to share any confidential data. Useful information includes:

- The Splunk products and versions you're using
- Whether or not you're using forwarders, and which type(s)
- Error messages you're seeing, and in which logs
- Examples of the data you're indexing or searching (if relevant to your problem)
- Configurations, regexes, etc.
- Prior research you have done and your desired result
- Exact Splunk Enterprise terminology

The text editor tools are your friend. Use the Code Sample button to wrap any sample code, data, search strings, or conf file stanzas in a code box to render special characters properly. If you are including snippets of code within a sentence, enclose it with back-ticks (`).
Resolving your post

After you receive an answer with a working solution to your question, please resolve your post by clicking "Accept" directly below the answer that solved your problem. This will make it easier for other users with the same issue to find the solution when searching for answers.

How to answer a question

If you have a full, complete answer for a question, use the Enter your answer here? text field at the bottom of a question page to fill out and submit your response.

If you still need to gather more information from the poster of the question before proposing a thorough solution, click Add comment directly below the question to communicate what you need them to provide.

Be thorough and explain why your solution answers the question. Educate the community on how to troubleshoot and solve the problem rather than simply copying and pasting an answer.

Provide links

Make it easy for the reader to find what is needed and point them in the right direction from the start.

If your answer touches on a topic covered in the Splunk documentation, you should add a reference link so users can explore more information on the subject. If there are external resources such as regex helper tools or Wikipedia, provide links to the tools/site if the information on those links support your answer.

Tips for getting your questions answered

If you can't find what you're looking for, then follow these best practices for asking a question. These recommendations are based on observations of the interactions between askers and answerers, as well as research conducted on common factors found in questions that do not receive any answers.

Search first

Before asking a question, you should search the Splunk documentation. The documentation is a great first resource for answers to your questions. If you don't
find what you are looking for, then search Splunk Answers to see if someone else has asked the same or similar question.

If you feel like you are not getting the best relevant results from the built-in search on Answers, use Google to search. Run the search with "answers.splunk.com" and with all of keywords for what you are searching for.

Make sure you use Splunk terms in your searches for better results!

**Posting questions**

Ask only one question for each Splunk Answers post. Keeping your questions streamlined improves the likelihood of getting an answer quickly.

Post questions when the traffic on the site is at it's highest. Typically, this is during business hours, Monday through Friday, US Pacific Time.

**Titles used for questions are key**

The title that you use for your questions are important because it is the first and only thing that users see in a list of questions.

The question title should clearly state what you are asking for help with. This helps subject matter experts filter and find which questions are worth volunteering their valuable time to answer.

The following list contains examples of good question titles:

- How to set the x-axis limits of a line chart?
- Why is our universal forwarder not forwarding all logs on DHCP servers?
- How to add a column of averages to a timechart?

Be brief but specific in your question titles.

**Details, details, details**

To increase the chances of getting your questions answered, provide as much detail about your environment and the issue you are having. This saves time and helps eliminate a lot of back and forth clarification comments for the people trying to help you.

Some of the information you should provide includes:
• What Splunk products and versions are you using?
• Use exact Splunk product names and terminology because it make the content searchable for everyone. If you are not sure about the exact names and terms to use, see the Splexicon.
• What type of Splunk deployment that you are using. Standalone, distributed search, indexer clustering, search head clustering, and so forth.
• Are you using forwarders? Which type? Which version?
• Include any relevant configuration file names, stanzas, and settings.
• What error messages are you seeing? In which logs? On what Splunk instances?
• What searches or regular expressions did you use?
• Show what prior research you have done into the issue, so other users don't repeat the steps you have already taken to troubleshoot your issue. Be respectful of the time that other people have volunteered to take to help you. It is not the volunteer's job to do your homework for you.

The more information that you provide, the more likely your question will be answered quickly.

**Sample data and expected results**

If applicable, provide anonymized sample data. Having sample data to work with is helpful for troubleshooting, parsing, field extractions, search syntax, and so forth.

One of the most important things to use is the Code Sample button when you are sharing any sample data, code, searches, regular expressions, and so forth. This will ensure that special characters render properly.

If possible, show an example of what you expect the outcome or results to be. Knowing what you expect helps other users propose options for producing that outcome or results.

**Tagging your questions**

Tagging your questions can increase the chances that the people most knowledgeable about your issue see your question. Splunkers and Splunk users can follow specific tags to receive notifications when a question is posted with those tags.

• You can select which Splunk product your issue is related to and this is added to the list of tags for your question.
• Make sure to add tags for key Splunk terminology. Splunk terminology is documented in the Splexicon.
• If you are using apps or add-ons, it is important to tag questions with the correct names for the apps and add-ons from Splunkbase.

Use tags to search and categorize

Answers uses tags to help categorize content for easier searching. For example, an Answer about setting up SSL forwarding with self-signed certificates might be tagged with the words ssl, forwarding, and security.

A list of the more popular tags currently in use is shown on the right side of the Answers landing page. Click on any tag to instantly search for all Answers tagged with that tag.

For a complete list of all tags currently defined in Splunkbase, click the Tags tab in Splunk Answers. You can then sort alphabetically by name or by popularity.

Email notification

You can tell Answers to send you an email if someone posts an Answer tagged with a tag you specify. For example, you might be interested in knowing when someone posts a question or answer about a particular technology you work with.

To set up email notifications:

1. Log into your splunk.com user account.
2. Navigate to the Answers landing page.
3. Click on the Tags tab, and search for the tag you want to follow.
4. Select your desired tag from the results, and click +Follow on that tag’s page.

To stop receiving notifications for a tag, navigate to that tag’s page and click Unfollow.

Follow content and users

All users have the option to follow content in the areas that they are interested in. You can follow a specific question, or you can follow a topic (tag). You can also
follow other users to stay up-to-date on their latest Splunk Answers contributions. Following experts who post high quality content is a great way expand your Splunk software knowledge.

**Follow a question**

When you follow a question, you receive an email notification whenever there is any follow-up activity on that post such as a new comment, answer, or accepted answer.

1. To follow a question, click the green **Follow** button on the right side of the question page.

**Follow a topic (tag)**

To stay up-to-date with the latest questions that are posted about a specific topic, you can follow a topic. You receive an email notification whenever a question is posted to a topic with that tag.

For example, if you are interested in questions that are asked about the HTTP Event Collector, you can follow the http-event-collector topic.

1. To follow a topic, click the tag. A page appears that list the posts to which that tag is assigned.
2. Click on the **+Follow** button at the top of the page, above the **Ask a question** button.

If you’d like to explore all of the tags that exist on the site, or you would like to search for certain tags to follow, click the **tags** tab on the right side of the header on any page in Splunk Answers.

**Follow a user**

You can follow when a user posts something in Splunk Answers. You will receive an email notification whenever that user creates or responds to a post.
There are a couple reasons to follow other users:

- The top contributors on Splunk Answers have the highest karma points and K/P ratios because they are both smart and helpful. There is much to be learned from the knowledge and high quality posts of these champions in the Splunk community. Users see this as a great way to learn from the very best.
- You might have colleagues in your organization on Answers and you want to stay updated on what issues they are trying to solve.

There are two ways you can follow another user:

1. Hover over the user's profile image or username and click the +Follow button in the displayed pop-up.
2. If you are already viewing a user's profile page, you can click the Follow This User button on the profile page.

Voting etiquette

Some of our most active members on Answers have helped set the standard of how voting etiquette should work in the Splunk community, which distinguishes and sets our culture apart from other Q&A forums. We want to promote a positive and constructive learning environment as much as possible. Users should be encouraged to grow with and educate one another instead of feeling fear if they contribute in the forum.

Follow these voting etiquette guidelines when engaging with other users on Splunk Answers.

Upvoting

Upvote questions, answers, and comments as soon as possible to give credit where it's due for high quality posts. If a user posted an awesome answer to your question, upvote the answer in addition to accepting it.

When to upvote and when not to

Use the upvote feature strictly for acknowledging useful responses and for giving recognition to users who helped you solve your problem. Only upvote a question, comment, or a solution for the following reasons:
It helped you solve your own problem.
• It's something that you agree with.
• It's an example of a positive interaction in the community.

These are good reasons to upvote someone.

A bad reason to upvote a user is just because they are your co-workers, friends, or family.

**Karma gaming is prohibited**

Also, please be cool. Any sort of karma gaming is prohibited. Karma gaming activities include but are not limited to the following:

• Creating a separate Answers account with the purpose of upvoting your own answers.
• Crowdsourcing friends and coworkers to upvote your Answers posts.

Engagement in such behavior will result in warnings, loss of karma points, and eventual suspension of the Splunk Answers accounts in violation.

**Downvoting**

Downvoting should be reserved only for posts proposing solutions that could potentially be harmful for a Splunk environment or goes completely against known best practices.

• If an attempted answer does not solve your question, simply commenting with constructive feedback and why it didn't work is more beneficial for the community to learn from.
• Downvoting people who are genuinely trying to help you does not make the situation any better and might deter experts from addressing your questions in the future.

**How voting etiquette developed**

If you’re interested in seeing how this voting etiquette was developed, check out this Splunk Answers post:
ME TOO feature

The ME TOO feature enables users to identify a question or problem that is something they are interested in seeing a solution to.

When you are logged in to Splunk Answers, the ME TOO button is visible on the left hand side of every question. Clicking the ME TOO button subscribes you to the post. You will receive updates whenever there is a comment or or other activity on the post.

The number of users who have clicked the ME TOO button is displayed under the question. This helps to identify that there are multiple users interested in finding a solution to the same problem.

Benefits of the ME TOO feature:

- Helps subject matter experts in the forum identify which posts are most pressing to other users. This helps the SMEs focus on the posts that they should contribute their time and efforts to.
- Reduces the number of duplicate posts with similar problems.
- Highlights answers and users who provide great content.
Karma and leaderboards

What is Karma?

On the Splunk Answers and Splunk Apps sites, karma is something you earn by participating in the Splunk community: contributing thoughtful answers and comments to people's questions, uploading apps, etc. Karma points provide a rough measurement of your reputation in the Splunk community and how much the community trusts you.

For example, if you ask an interesting question or give a helpful answer or comment, your input will be upvoted. When a question or answer is upvoted, the user who posted it will gain some points, which are called "karma points".

On the other hand if the answer is misleading, it will be downvoted. Each vote in favor awards you 15 karma points, each vote against subtracts 5 points from your total.

Posting an app is a great way to build 'instant karma' (haha), giving you 100 points for every app and add-on you upload. Check out "About submitting content" in the Apps manual to learn more about submitting apps and add-ons.

When you register and verify your email address on Answers, you start with 20 karma points, enough to ask two questions a day, upvote questions or answers, or comment on questions or answers.

As you earn more karma, you're given more powers on Answers. With enough karma, you can add tags to posts, edit other users' posts, restructure Answers postings, close and delete spam or duplicate postings, and more. Our users are what makes this site great, and we trust you to help maintain its awesomeness.

Check out the rewards table to see how much karma is needed to earn various privileges.

Karma Post ratio

Karma Post (K/P) ratio is a number that measures the quality of a user's contributions on Splunk Answers.

A user's K/P ratio is calculated using their total karma points divided by the total number of posts by that user which includes questions, answers, and comments.
KP ratio = total karma points / total number of posts

You can find a user’s K/P ratio in that user’s profile under their profile image.

How to earn Karma on Answers

You gain or lose karma on Answers by posting and voting. The following are the current karma rules:

<table>
<thead>
<tr>
<th>Activity</th>
<th>Karma gained (+) or lost (-)</th>
</tr>
</thead>
<tbody>
<tr>
<td>A user accepts your answer</td>
<td>+20 points</td>
</tr>
<tr>
<td>You accept an answer posted to your question</td>
<td>+2 points</td>
</tr>
<tr>
<td>A user upvotes your answer, question, or comment</td>
<td>+15 points (maximum 200/day)</td>
</tr>
<tr>
<td>A user downvotes your answer, question, or comment</td>
<td>-5 points</td>
</tr>
<tr>
<td>You downvote a user’s answer, question, or comment</td>
<td>-1 point</td>
</tr>
</tbody>
</table>

Karma rewards

When you first register on Answers, you start with 20 karma points, which is enough to post two questions a day, answer questions, comment, and upvote. As your posts are upvoted, and your answers accepted, you gain karma as described in the previous section. Note that some activities lower your karma (for example, downvoting). If your karma total drops below 3 karma, you won’t be able to upvote.

<table>
<thead>
<tr>
<th>Activity</th>
<th>Karma required</th>
</tr>
</thead>
<tbody>
<tr>
<td>upvote a question, answer, or comment</td>
<td>3</td>
</tr>
<tr>
<td>Like a comment</td>
<td>10</td>
</tr>
<tr>
<td>Flag a question, answer, or comment</td>
<td>15</td>
</tr>
<tr>
<td>Skip captcha</td>
<td>22</td>
</tr>
<tr>
<td>Post links</td>
<td>50</td>
</tr>
<tr>
<td>Attach files</td>
<td>60</td>
</tr>
<tr>
<td>Edit question tags</td>
<td>100</td>
</tr>
<tr>
<td>Activity</td>
<td>Karma required</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Convert own answer to a comment</td>
<td>100</td>
</tr>
<tr>
<td>Convert own comment to an answer</td>
<td>100</td>
</tr>
<tr>
<td>Downvote a question, answer, or comment</td>
<td>100</td>
</tr>
<tr>
<td>Close own question</td>
<td>250</td>
</tr>
<tr>
<td>Edit any question, answer, or comment</td>
<td>1000</td>
</tr>
</tbody>
</table>

**About the leaderboards**

Visit the **users** tab, to display the leaderboards:

- By default, you see your own entry and ranking in the *quarter to date* leaderboard. The *quarter to date* leaderboard shows performance by Splunk Answers community members during the current quarter, including current rank for the quarter, change in rank, karma earned this quarter, and most recent activity.
- You can also switch to see the *all time* leaderboard. The *all time* leaderboard shows your current ranking and performance for the entire period of time you've been a member of the Splunk Answers community.

The **quarter-to-date** leaderboard is updated every 30 minutes on the half-hour.

If your karma score is tied with one or more other users, your ranking is determined by how recently you have been active on Splunk Answers.

We'll be launching some karma competitions soon, so check the leaderboards often!