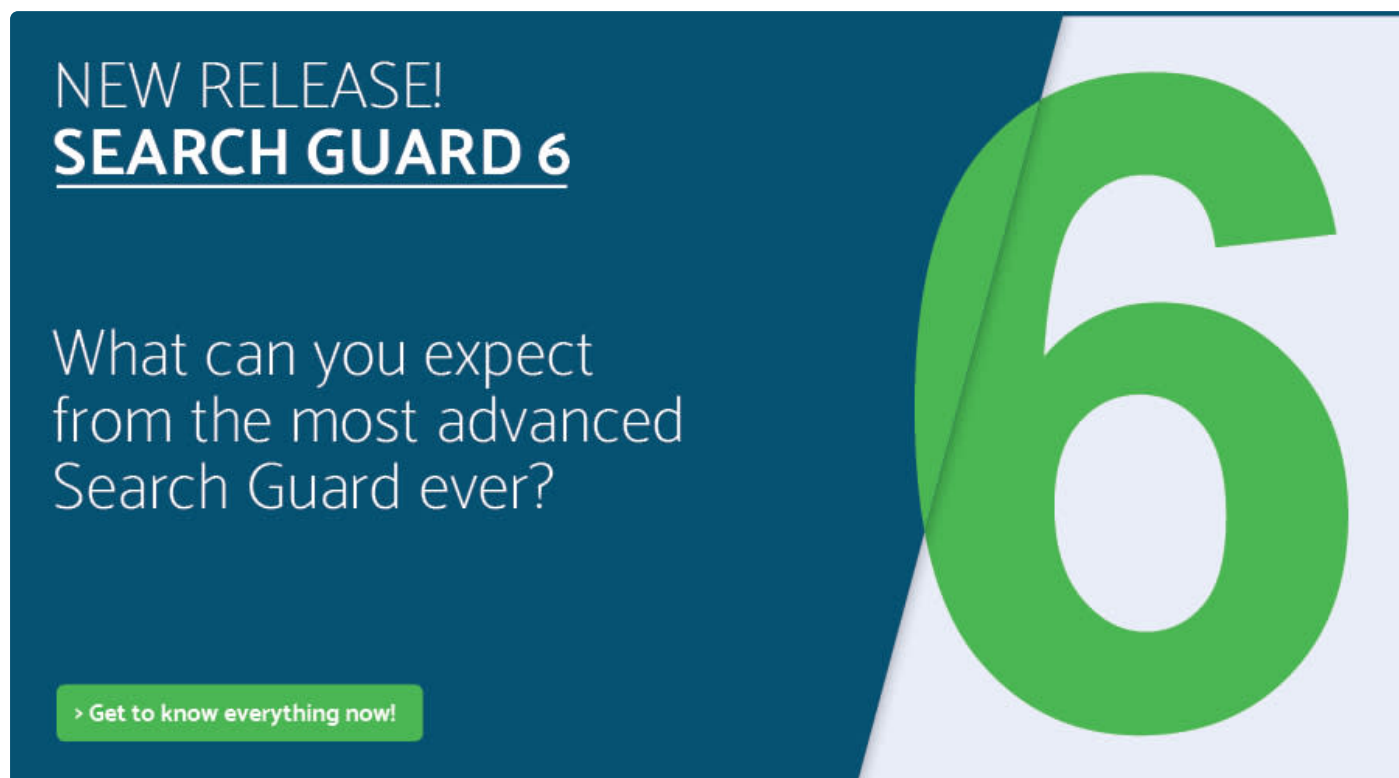


Search Guard 6 is coming!

Claudia Kressin · 2017-08-21



What a ride! It's only one year since we officially released Search Guard, and the feedback we got from customers and the community has been overwhelming already. So, first of all, thank you for your input and your help in making Search Guard the best security solution for Elasticsearch out there!

The last year was a very busy one: We've worked on new features and new releases, developed our own Kibana plugin, added multi-tenancy, improved the documentation and implemented a lot of feature requests and improvements. The Search Guard code has been audited by customers multiple times, and we're very proud that the number of issues has been incredibly low over the course of the year.

On our way to Search Guard 6

Elasticsearch 6 is already on the horizon, and so is Search Guard 6! Since this is a major version upgrade, we have the opportunity to introduce bigger changes, while at the same time ensuring backward compatibility with Search Guard 5.

Offsite and roadmap

So we've brought together the Search Guard team and discussed the next major Search Guard version intensively on a strategy offsite. We had a ton of information, feedback and feature requests in our hands, so the backlog of Search Guard 6 filled quickly. However, there were two main points that showed up repeatedly:

- Generating certificates and setting up TLS is difficult

- Understanding the configuration and the usage of sgadmin is difficult

Easing the use of TLS

Let's face it, TLS was never an easy topic. But we strongly believe that it's the best way to secure your Elasticsearch traffic, both on HTTP and on the transport layer. We will definitely stick with our initial decision to make TLS mandatory on the transport layer, because without it, all other security efforts are pretty much in vain. In our view, allowing unsecured traffic on the transport layer was never an acceptable behavior for a security product, and [relying on firewalls and proxies for security is always a bad idea](#).

At the same time, we want to make it easier for you to quickly try out all Search Guard features. And deal with the nitty-gritty TLS details later when you move into production.

At the moment the quickest way to set up Search Guard is to:

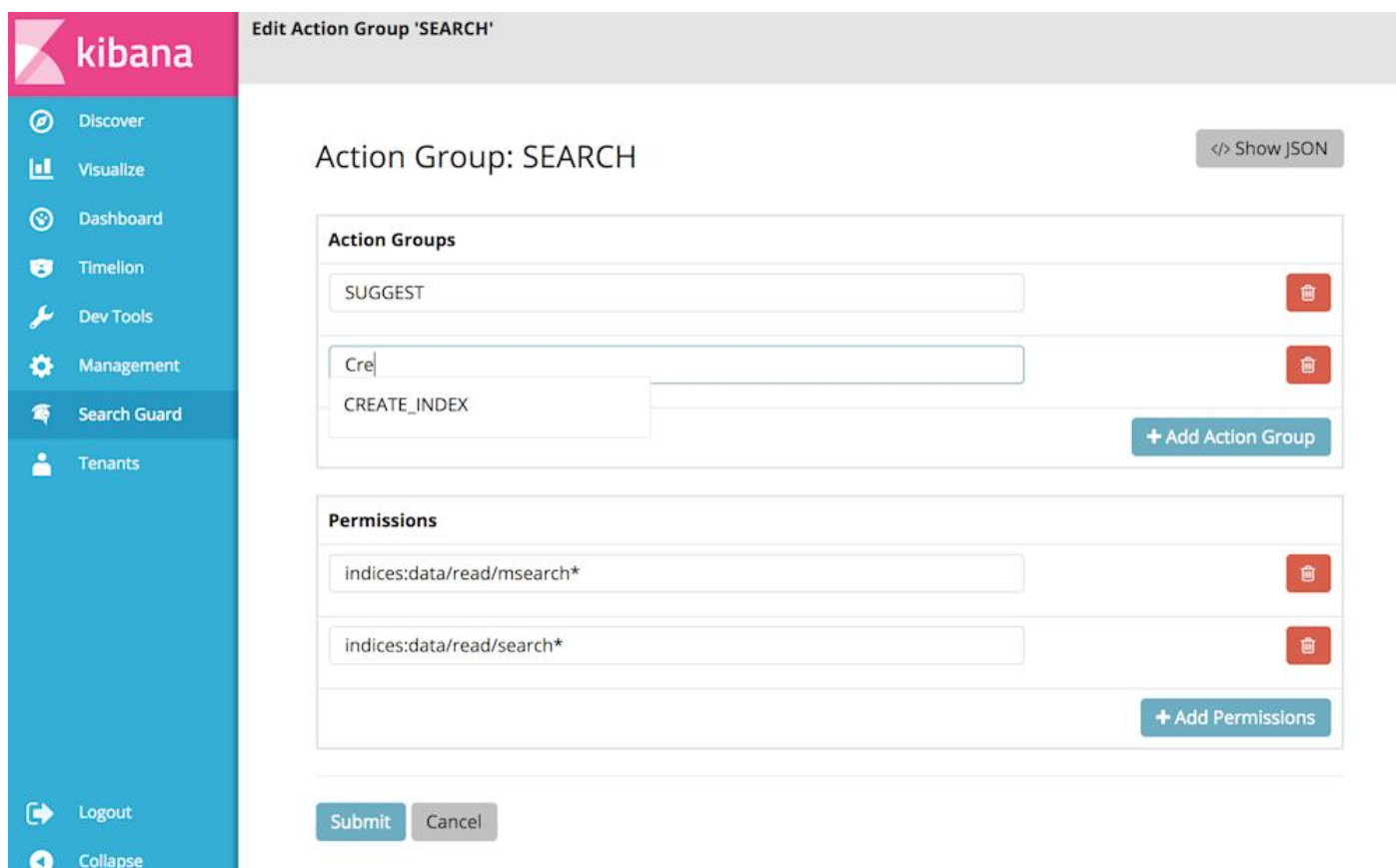
- Install the Search Guard plugin
- Execute the demo installer
- Start up Elasticsearch
- Execute the sgadmin demo script to initialize the configuration index

Search Guard 6 will ship with an installer which will automate the setup and configuration process completely. You just need to install the plugin, start Elasticsearch and will have a working environment right away! Generating and installing your own certificates will still be required for production systems, however.

Configuration GUI

The Search Guard configuration is based on a bunch of yaml files which get uploaded to the configuration index with sgadmin. This is great for automating the installation process via Puppet, Ansible or Chef since everything can be scripted. The downside is that you need to understand the content and structure of the configuration files before you're able to make any changes. We've finally decided to provide you with a Kibana-based configuration GUI which will make it super easy to view, edit and save all configuration settings.

The initial release of the GUI will be exactly that – a tool for managing the Search Guard configuration. But our plan is to add more useful features in future so that the GUI will be your one-stop-shop for everything Search Guard.



Early preview of the upcoming Search Guard configuration GUI.

Backwards compatibility

There are many other features we have on our roadmap. For example, shipping Search Guard with all enterprise modules already installed. At the same time, we will take extra care not to break any installation or configuration processes you already have in place. So, in this case, we will continue to publish the modules individually on Maven Central, as it is now. All your scripts and automated processes will still work with Search Guard 6.

We will continue to maintain and support all existing features of Search Guard 5. The only exception is features that Elasticsearch is going to deprecate:

- Document types are going away
 - In Elasticsearch 6, it will not be possible to create more than one document type on any index
 - Indices created with Elasticsearch 5 containing multiple document types will still be supported
- Tribe nodes will be replaced by Cross Cluster Search
 - We will continue to support tribe nodes, but advise users to move to Cross Cluster Search instead

Keeping Search Guard the best security suite for Elasticsearch

Our aim is to keep Search Guard the best security suite for Elasticsearch available. Our main focus is and will always be security. We understand the current state of security as well as new requirements that the

future will bring. Search Guard 6 will come with many other features and improvements which will boost security on all levels.

Conclusion

We're very much looking forward to Search Guard 6. With the features described in this blog post and some more goodies that lurk in our back log, we think this release will be a major improvement regarding the Search Guard user experience.

This article was published on the Search Guard blog: <https://search-guard.com/blog/search-guard-6-roadmap/>
Search Guard is Security and Alerting for Elasticsearch and Kibana — search-guard.com · [Start a free trial](#)