Managing configurations in Splunk Cloud Platform

As a user of Splunk Cloud Platform, you want to automate configuration management as much as possible. However, Splunk Cloud Platform has fewer options for configuration management than Splunk Enterprise. The following methods are not available in Splunk Cloud Platform:

- Splunk Command Line Interface
- Direct editing of configuration files in the shell
- Direct access to indexers or the cluster management node via shell or API
- Some Splunk REST API endpoints (For more information, see REST API access limitations)
- Ability to install apps that require manual checks without a support case
- Classic: Ability to install apps on instances other than your primary search head without a support case

You need to understand what your options are now so you can have your Splunk Cloud Platform deployment configured as you need it.

It's still possible to automate configuration in Splunk Cloud Platform via app installation or API calls, and there are many existing Splunkbase apps and public Github projects that you can use as starting points. Whichever method you choose, there are a few best practices you should follow:

**Use apps**

- Whether you deploy using the API or App installation, organize managed configuration into apps.
  - Keep managed apps in a source control system and automate app vetting, testing, and packaging.
  - Don't allow write access to managed apps via the UI.
- Create separate apps in the Splunk UI for folks who want to develop unmanaged configuration in the UI.

**Use the correct API**

Admin Config Service (ACS) is a new API that allows you to manage:

- Firewall rules
  - Incoming IP allow lists
  - Outbound ports
- Victoria: HEC tokens
- Victoria: Indexes
- Private app installation

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.
In Classic Cloud, you can use the Splunk REST API to manage Indexes and HEC tokens.

**Migrate to the Victoria Experience when possible**

When you migrate from Classic Experience to Victoria Experience in Splunk Cloud Platform you can:

- Self-install most Splunkbase apps.
- Install all apps - both Splunkbase and Private - to all search heads.
  - All apps are installed to all search heads in Victoria. There is no way to install an app to a single search head.
- Manage inputs directly on the search head, which replaces the Classic inputs data manager.

**Next steps**

The content in this guide comes from a [Conf21 breakout session](https://example.com), one of the thousands of Splunk resources available to help users succeed. In addition, these Splunk resources might help you understand and implement this use case:

- Splunk 2021 BSides: [Integrate Splunk Cloud into your CI/CD pipelines](https://example.com)