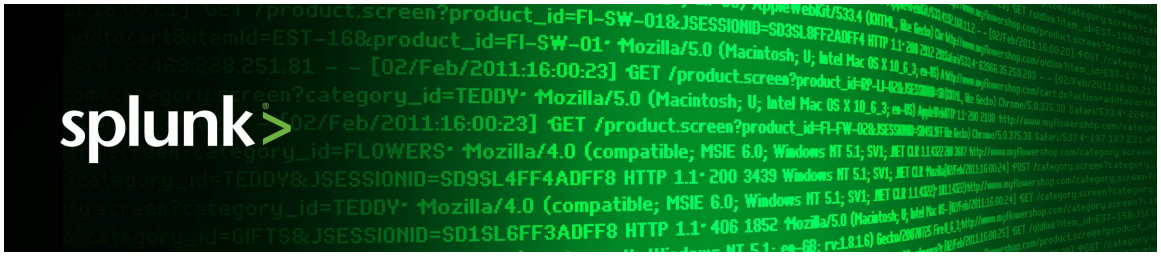

Splunk® Answers and Splunkbase Working with Splunkbase splunkbase

Splunkbase file standards reference table

Generated: 9/30/2016 6:21 am

Splunkbase file standards reference table

The Splunkbase team evaluates your submitted content to ensure it meets the following file standards.

Packaging and naming standards

Acceptance Criteria	Description
File format	File is tarballed with one of the following extensions: .tar.gz, .tgz, or .spl. If there are any other compressed archives within the main release that needs extracting, this must be made clear in release notes.
File suffix naming	File suffix is ".spl", ".tar.gz" or ".tgz". See *Package your app or add-on* in the Splunk Enterprise documentation for packaging information.
App description	The description is next to the app or add-on name in Splunkbase.
App icon	The icon should be in PNG format and 36px x 36px. Naming of icon is case-sensitive.
App screenshot	Upload a 623px x 350px screenshot or splash screen in PNG format.
File size	Any file greater than 200MB requires clarification for the reasoning for the large size.
Unnecessary files	Package can only includes files that the app needs. Example: Files from the developer's local build environment (such as local log files) that were inadvertently built into the release.
Root directory	Submitted app packages must only have one root folder, which is the folder that contains the Splunk app or add-on.
Local directory	Local directory is reserved for user preferences. Any files in the local directory must be moved to the default folder.

Splunk configuration file standards

Acceptance Criteria	Description
Application Descriptor	App.conf file is present, mandatory fields, launcher **description**, **author**, and **version** fields are filled in.
App ID field	

	The **id** field, found in app.conf, must fit Splunkbase naming guidelines (A-Z, 0-9_-.), match the ID and root folder of your app, and must not be already used by another application (Example: id = dbx).
App label field	The app **label** field must exist in app.conf, and must meet Splunkbase's length requirements (5-80 characters).
App version field	The app **version** field, located in app.conf, must meet Splunkbase naming guidelines, and cannot match a previously used version of your application.
Application Updates	Application update is consistent in versioning/numbering with previous releases.
Directory placement	Conf files distribute in the default directory. Local directory, if it exists, is empty.

Splunk XML file standards (if applicable)

Acceptance Criteria	Description
Simple XML	XML is well formed
Advanced XML	XML is well formed
Setup XML	XML is well formed
Navigation XML	XML is well formed

Source code standards

Acceptance Criteria	Description
Compiled python files are not allowed	*.pyo and *.pyc files are not allowed by Splunkbase.
Hidden files	Files that start with . (Example: .DS_Store) are not allowed.

Binary content standards

Acceptance Criteria	Description
Misplaced executable scripts	Put all scripts (.py, .sh, .bat etc..) and .exe files in the bin directory.
Binary content	Any binary content is what it purports to be (for example, an image is an image, a compiled library is required, a pdf is genuinely a pdf etc.)

Splunk version support and installation standards

All submitted apps must run on the versions of Splunk that your app claims to support.

Operating system standards

Acceptance Criteria	Description
Hard coded paths	No hard-coded filepaths in scripts relative to author's local developer environment.
Executable files	Files that are executable actually need to be executable.
User privileges	Scripts must not maliciously attempt to switch into other user accounts, create new users, or run sudo.
Malicious Commands	No use of malicous commands designed to corrupt the OS or Splunk instance, for example: • rm -rf • kill -9 • shutdown , halt
File system writes	Calls to open/popen are checked to determine where a file is being written to.

Malware/viruses, malicious content, user security standards

Acceptance Criteria	Description
Check for malware/viruses	Run scanner software to check for viruses and malware.
Check for offensive material	No offensive material is in the distribution (pornography, racist content etc.).
Check embedded links	Any URL links in the app do not link to malicious or offensive sites.
Authorization credentials	No plain text authorization credentials are in the app artifacts.
Hostname/IPs	No sensitive hostnames/IPs are left in the distributed app.
Invasive relative paths	Relative paths included in the tarfile that are invasive (Examples: ../README.md or default/../appserver/static). will prevent your app from Splunkbase approval.

External data sources

The application's publisher must document if the app calls an external source for data or other info.

Documentation standards

Acceptance Criteria	Description
Basic README	Package your app with a simple README which includes version support, system requirements, installation, configuration, troubleshooting and running of the app.
Language	Deliver core documentation in English.
Editing/Proofreading	Check that your documentation is free of major editing and proofreading (spelling, grammar, punctuation) issues.

Support standards

Contact information (email, link to a ticket system, etc.) for application support is provided in the documentation or app's web content.

Intellectual property standards

If you are using the Splunk logo, its usage must meet Splunk branding guidelines.