Splunk® Supported Add-ons Splunk Add-on for ServiceNow released

Set up the Splunk Add-on for ServiceNow

Generated: 4/23/2018 11:15 am

Set up the Splunk Add-on for ServiceNow

You can configure the Splunk Add-on for ServiceNow through Splunk Web or by modifying the `service_now.conf` configuration file. If your Splunk platform deployment is distributed, you must perform these setup steps on your data collection nodes (usually one or more heavy forwarders) and on your search heads. Search head configuration is only necessary if you want to perform push integration from search commands, alert actions, and alert-triggered scripts.

If you are using this add-on with a search head cluster, perform these setup steps on one search head node in Splunk Web. The cluster syncs the settings to your other nodes. Click **Settings > Show All Settings** to see the set up link on your search head cluster node.

Set up the add-on using Splunk Web

Set up the add-on in Splunk Web.

1. In Splunk Web, click **Apps > Manage Apps**.
2. In the row for Splunk Add-on for ServiceNow, under **Actions**, click **Set up**.

   If you don't see the **Set up** link, see Cannot access setup page.
3. In the ServiceNow Setup section, provide the URL for your ServiceNow environment. Your ServiceNow URL should not end with any special characters. Remove any trailing slashes.
4. Enter your **User name** and **Password**. If you configured ServiceNow to integrate with the Splunk platform, use the same username that you configured during the integration for this setup step. If you did not perform this configuration, use an account that has read-only permissions to the database tables from which you want to collect data.
5. If you are using a proxy, check **Enable Proxy**, and complete the ServiceNow Proxy Setup section. Unchecking the box deletes all proxy settings.
6. Enter the **URL**, **port**, **username**, and **password**.
7. If you are using the proxy to do DNS resolution, check the box next to **Use proxy to do DNS resolution**.
8. Select the correct **Proxy type** from the list.
9. In the ServiceNow Data Collection Setup section, configure the fields only on your data collection node(s):

   - **Collection interval** is how frequently the add-on pulls the data from a database table. The default is 120 seconds.

- **Data started from** sets the point of time from which the add-on collects the data from the database table. The default setting is **one year ago**.
- **Logging level** supports debugging. If you encounter issues with the add-on, enable "DEBUG" level logging to help troubleshoot.

If you have multiple search heads that are not in a search head cluster, perform all the same steps on each search head to support search-time push integration. Configure data collection only on your data collection nodes, typically one or more heavy forwarders.

Set up the add-on using the configuration file

Set up the add-on using the `service_now.conf` configuration file.

1. Go to `$SPLUNK_HOME/etc/apps/Splunk_TA_snow` and a directory called `/local`, if it does not already exist.
2. Copy `Splunk_TA_snow/default/service_now.conf` to `$SPLUNK_HOME/etc/apps/Splunk_TA_snow/local`.
3. Configure the values using the following table.

Stanza	Argument	Description
`[snow_default]`	`collection_interval`	How frequently the add-on issues API requests to collect the data from a database table. Default is 120 seconds.
	`priority`	Used by the job scheduler.
	`record_count`	The maximum number of records to query back from ServiceNow each time. The value must be larger than 0. Default is 5000. ServiceNow recommends the count not exceed 10000, otherwise there may be performance issues.
	`loglevel`	The verbosity of the logs.
	`since_when`	The UTC timestamp in YYYY-MM-DD hh:mm:ss format at which the add-on begins to collect the data from

		a database table, ignoring any older data in the database table. The default is one year ago.
	`url`	The URL of your ServiceNow instance.
	`release`	The version of ServiceNow you are running. Enter `Automatic` to trigger the add-on to auto-detect the version for you.
`[snow_account]`	`username`	The username of the account that the Splunk platform uses to connect to ServiceNow. If you configured ServiceNow to integrate with the Splunk platform, use the same username that you configured during the integration for this step. If you did not perform this configuration, use an account that has, at minimum, read-only permissions to the database tables from which you want to collect data.
	`password`	The password of the ServiceNow account the Splunk platform uses to connect to ServiceNow.
	`proxy_enabled`	Indicates whether connection to ServiceNow occurs through a proxy. Default is false.
	`proxy_url`	URL or IP address for the proxy connection. Invoked only if `proxy_enabled` is set to true.
	`proxy_port`	Port for the proxy connection. Invoked only if `proxy_enabled` is set to true.
`[snow_proxy]`	`proxy_username`	Username for the proxy connection. Invoked only if

	`proxy_enabled` is set to true.
`proxy_password`	Password for the proxy connection. Invoked only if `proxy_enabled` is set to true.
`proxy_rdns`	Default is `0`. If you use the proxy to do DNS resolution, set to `1`.
`proxy_type`	Default is `http`. Other accepted values are `http_no_tunnel`, `socks4`, and `socks5`.

4. Save your changes.
5. Restart your Splunk instance.

The following example shows a sample `local/service_now.conf`.

```
[snow_default]
collection_interval = 120
priority = 10
record_count = 5000
loglevel = INFO
since_when = 2000-01-01 00:00:00

[snow_account]
url = https://my.service-now.com/
release = Eureka
username = admin
password = admin

[snow_proxy]
proxy_enabled = 1
proxy_url = 10.5.6.7
proxy_port = 8081
proxy_username = splunk
proxy_password = splunk
proxy_rdns = 0
proxy_type = http
```

If you have multiple search heads that are not in a search head cluster, perform all the same steps on each search head to support search-time push integration. Configure data collection only on your data collection nodes, typically one or more heavy forwarders.