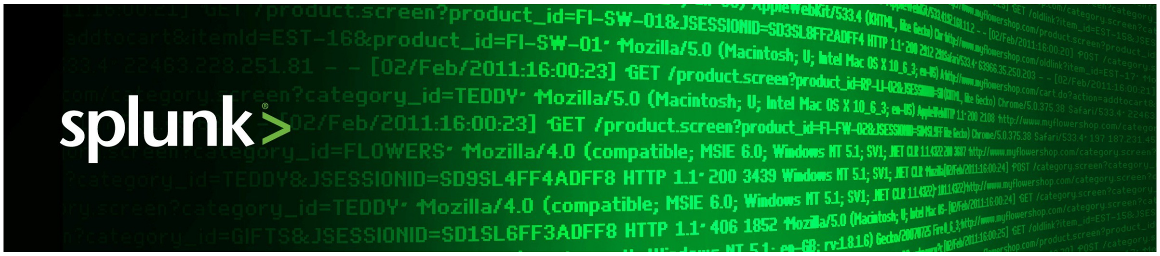

Splunk® Supported Add-ons Splunk Add-on for ServiceNow released

Configure ServiceNow to integrate with the Splunk platform

Generated: 4/29/2018 8:08 pm

Configure ServiceNow to integrate with the Splunk platform

If you want to enable users to create incidents and events in ServiceNow using the custom generating search commands, custom streaming search commands, or alert-triggered scripts, integrate ServiceNow with your Splunk platform instances. The way you perform this integration depends on the version and deployment of your ServiceNow instance.

Follow the guide that matches your version and deployment of ServiceNow.

Version	ServiceNow deployment	Instructions
Geneva, Helsinki, Istanbul, Jakarta, and Kingston	ServiceNow in the cloud	Apply the integration application
Geneva, Helsinki, Istanbul, Jakarta, and Kingston	ServiceNow bare metal installation on-premises	Use an update set

Prerequisite: If you want to perform push integration with the ServiceNow Event table, you must have the Event Management plugin installed and enabled before you proceed. See Hardware and software requirements for details about which features require this additional plugin.

See custom generating search commands, custom streaming search commands, and alert-triggered scripts, to learn more about integrating ServiceNow with your Splunk platform instances.

Apply the integration application

Download the Splunk Integration application from the ServiceNow app store and configure it.

1. Navigate to the ServiceNow app store and search for the Splunk Integration application.
2. Download the Splunk Integration application.
3. Deploy the Splunk Integration application on your ServiceNow instance.
4. Log in to your ServiceNow instance as an administrator.
5. Create the service account with the same user name you defined in the add-on setup. For example, `splunk_user`.
6. Assign the user the role of `x_splu2_splunk_ser.Splunk`.
7. (Optional) If you want to use the deprecated syslog table input, create an additional access control rule granting read-only access to the syslog log entry.

8. (Optional) In the **Requires Role** section, enter `x_splu2_splunk_ser.Splunk`. This grants your user read-only access to the syslog database table, which is otherwise only readable by administrators.
9. (Optional) Repeat steps 7 and 8 for `sys_audit`, `sys_audit_delete`, `sysevent` and `syslog_transaction tables`.
10. (Optional) If you want to use `sys_choice` table input, update the " sys_choice.* " access control of the table, by adding `x_splu2_splunk_ser.Splunk` role in **Requires Role** section.
11. (Optional) Repeat steps 7 and 8 for any additional database tables that you want to index.

Use an update set

The Splunk Add-on for ServiceNow includes several Update Set XML files in `$SPLUNK_HOME/etc/apps/Splunk_TA_snow/forExport`. Use the one that matches the version of ServiceNow that you are running.

You can download the update set file from the following locations:

- Update Set for Jakarta
- Update Set for Geneva, Helsinki and Istanbul

Install the file that matches your version on your ServiceNow instance

1. Log in to your ServiceNow instance as an administrator.
2. Navigate to **User Administration** to temporarily elevate your privileges to include the `security_admin` role.
3. Navigate to **System Update Sets**.
4. Follow the instructions in the ServiceNow documentation to apply the Update Set. Refer to http://wiki.servicenow.com/index.php?title=Saving_Customizations_in_a_Single_XML_File and http://wiki.servicenow.com/index.php?title=Transferring_Update_Sets for detailed instructions.

   If you see the error "Could not find a record in sys_report referenced in this update", you can ignore it.
5. Create the service account with the same user name you defined in the add-on setup. For example, `splunk_user`.
6. Assign the user the role of `Splunk`. Applying the `Splunk` role grants the `itil` role.
7. (Optional) If you want to use the deprecated syslog table input, create an additional access control rule granting read-only access to the syslog log

entry.

8. (Optional) In the **Requires Role** section, enter `Splunk`. This grants your user read-only access to the syslog database table, which is otherwise only readable by administrators.
9. Repeat steps 7 and 8 for any additional database tables that you want to index.