Meshlet Configurations for Splunk

Gold

To enhance your DataSync integration for **Splunk Enterprise**, you can optionally configure the Splunk meshlet to the directives listed below:

Directive	Description

ackUrl	Represents the Splunk URL for enabling indexer acknowledgement
	`splunk:`
	`  ackUrl: http://splunk-url/services/collector/ack`
	`  requestChannel: a7175f62-d67b-4793-a172-c1b946c0e444`

requestChannel	Represents a channel to be used with indexer acknowledgement.
	blocked URL **NOTE:** This configuration is to be used with the **ackUrl** configuration.
	`splunk:`
	`  ackUrl: http://splunk-url/services/collector/ack`
	`  requestChannel: a7175f62-d67b-4793-a172-c1b946c0e444`

saveInEvent	By default, data is saved into Splunk where the event name is the **name** field of the outbound message such as **incident.bulk** and the fields of the shared record are saved as fields in the Splunk event. However, when **saveInEvent** is enabled, all the data for the record's fields will be saved in the **Event** name instead. See View your event collections in Splunk for more details.
	`perspectium:`
	`  message:`
	`  inboundQueue: psp.in.meshlet.splunk.yourinstance`
	`  outboundQueue: psp.out.meshlet.splunk.%s`
	`  errorQueuePattern: psp.out.meshlet.splunk.error.%s`
	`  saveInEvent: true`

sourceType	A value for the source type of each record saved into Splunk. You can specify to use the table name of an incoming record by adding the **$table** value in **sourceType**. For example, if you send incident records and specify the **sourceType** configuration as **snow $table**, each incident record will be saved with a source type value of **snow incident**.
	`perspectium:`
	`  splunk:`
	`  url: http://3.46.13.38:8088/services/collector/event`
	`  authorizationHeader: " Splunk 0bfb9d66-8d5f-4fef-bae9-afa5a0642f21"`
	`  sourceType: snow:$table`

hideEmptyFields	Enable skipping empty field values of each record saved into Splunk. For example, with this configuration set as **true** and the meshlet receives an incident record with the field **assigned_to** empty, the **assigned_to** field will not be created when the record is saved into Splunk. If this configuration is not specified, the defaults value is **false** where empty fields are saved.
	`perspectium:`
	`  message:`
	`  hideEmptyFields: true`

Similar topics

- Generate a Splunk Event Collector token

Contact Perspectium Support

- Open Splunk HTTP Event Collector port to the Perspectium Integration Mesh
- DataSync for Splunk
- Get started with DataSync for Splunk
- View your event collections in Splunk

US: 1 888 620 8880

UK: 44 208 068 5953

support@perspectium.com