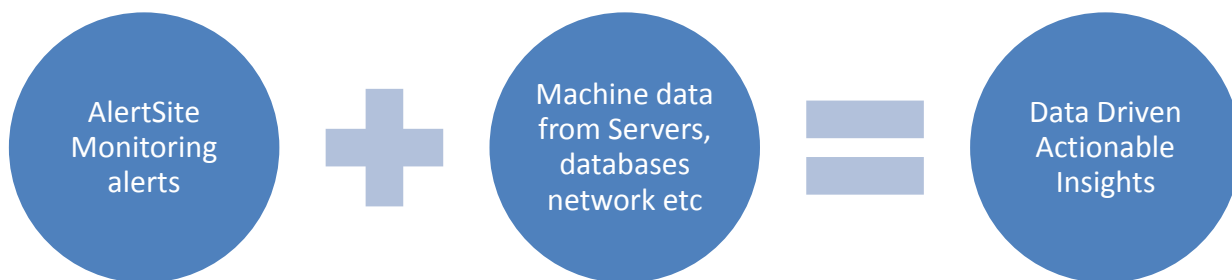


AlertSite – Splunk Integration

AlertSite has integrated with Splunk – a leading operational intelligence platform – to give you an effective way to correlate your application availability and performance issues with system log events.

Splunk collects and indexes machine-generated big data from infrastructure and applications such as websites, servers, databases, networks and custom applications, and provides search, analysis and visualization capabilities for that data.



AlertSite already has a highly sophisticated alerting system. Adding Splunk as an alert recipient on AlertSite, customers can send AlertSite monitoring information to their Splunk server to gain real time insight into business and IT metrics.

Requirements

- Splunk integration is available on AlertSite Enterprise (Usage-Based Monitoring) plans.
- You must be an AlertSite Admin or Co-Admin to configure the integration.
- AlertSite needs a user account to send data to Splunk. The account you can use depends on your Splunk edition.


If you use **Splunk Cloud** (paid subscription), contact Splunk Support and ask for the REST API credentials. This is the account you will need to specify in AlertSite.

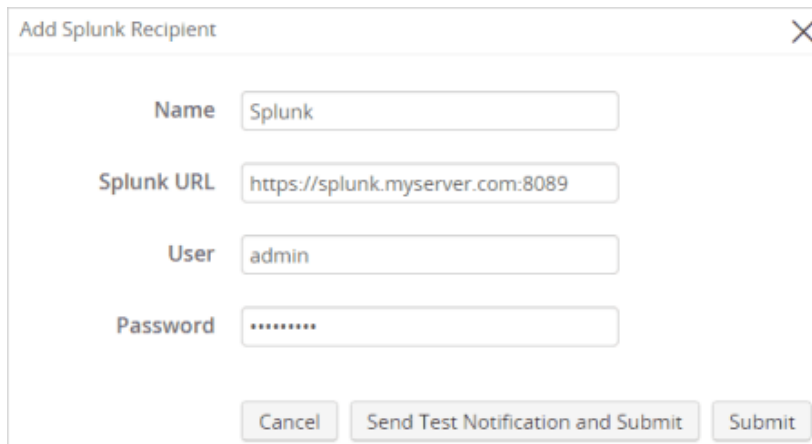
If you use **Splunk Light Free**, it supports a single administrator account and does not support additional user accounts. You will need to specify the admin account in AlertSite

If you use **self-hosted Splunk**:

- Your Splunk server must be accessible from the Internet.
- If Splunk is behind a firewall, the firewall must allow traffic on the Splunk management port (default is 8089). AlertSite locations send data to Splunk through this port

Add Splunk as an alert recipient in AlertSite

1. Log in to AlertSite UXM as an Admin or Co-Admin user.
2. From the top right menu, select  > **Manage Integrations**.
3. Click **splunk>** in the integrations list.
4. In the dialog that opens, click **New Recipient**.
5. Enter your Splunk server information.



Add Splunk Recipient

Name

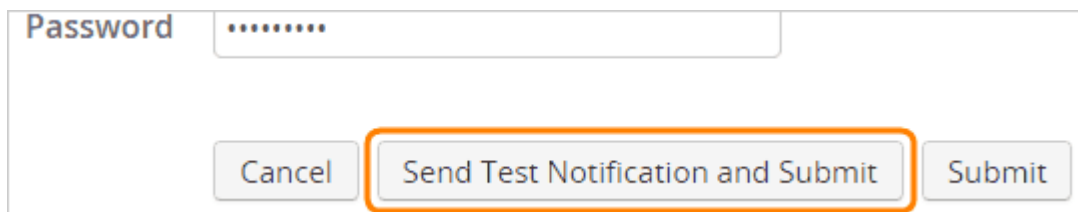
Splunk URL

User

Password

Setting	Description
Name	An optional display name for your Splunk server.
Splunk URL	Your Splunk server URL, including the prefix (<i>https://</i> or <i>http://</i>) and the Splunk management port (default is 8089).
User and Password	A user account on your Splunk server that will be used to post data to Splunk. This can be an admin account or any account with the <i>edit_tcp</i> capability

6. Click **Send Test Notification and Submit**. AlertSite will send a test alert to Splunk to verify connectivity.

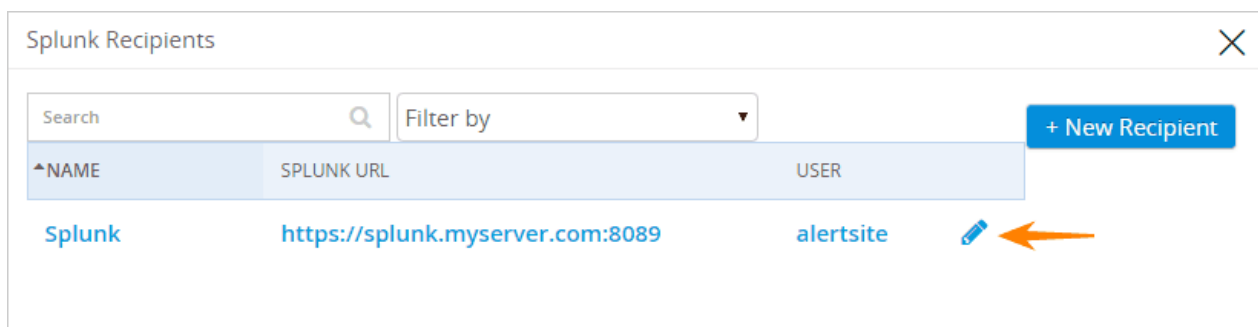


The screenshot shows a configuration window with a 'Password' field containing masked characters. Below the field are three buttons: 'Cancel', 'Send Test Notification and Submit' (which is highlighted with an orange border), and 'Submit'.

If the alert is sent successfully, you can find it in Splunk using the search string "sourcetype=alerts site test".

If an error appears, double-check your Splunk host name, port, login and password and try again.

7. After the previous window closes, click  next to the created recipient.



The screenshot shows a window titled 'Splunk Recipients' with a search bar and a 'Filter by' dropdown. Below is a table with columns: NAME, SPLUNK URL, and USER. The table contains one entry: 'Splunk' with URL 'https://splunk.myserver.com:8089' and user 'alerts site'. To the right of the 'alerts site' user is a pencil icon, which is pointed to by an orange arrow. A '+ New Recipient' button is in the top right corner.

8. Switch to the **Availability Alerts** tab. Select how many consecutive alerts to send to Splunk, and whether to send a "clear" notification. For a description of available settings, see [Recipient Properties](#).

The screenshot shows the 'Edit Splunk Recipient' dialog box with the 'Availability Alerts' tab selected. The 'Recipients' tab is also visible. The 'Availability Alerts' section is active, showing 'Enable?' checked, 'Alert after this # errors' set to 1, 'Stop alerting after this # alerts' set to 125, and 'Alert whenever an error clears' checked. At the bottom, there are buttons for 'Delete Recipient', 'Cancel', 'Send Test Notification and Submit', and 'Submit'.

9. To receive [performance alerts](#), switch to the **Performance Alerts** tab and enable them. Select which alert types to receive and whether to repeat successive performance alerts.

The screenshot shows the 'Edit Splunk Recipient' dialog box with the 'Performance Alerts' tab selected. The 'Recipients' and 'Availability Alerts' tabs are also visible. The 'Performance Alerts' section is active, showing 'Enable?' checked, 'Type' set to 'Warnings and errors' (selected with a blue dot), and 'Repeat successive performance alerts' checked. At the bottom, there are buttons for 'Delete Recipient', 'Cancel', 'Send Test Notification and Submit', and 'Submit'.

10. Click **Submit**.

That's it! Splunk is now ready to receive alerts from your AlertSite monitors.

Configure AlertSite Source Type in Splunk

You need to create a new source type in Splunk for AlertSite data so Splunk can properly parse AlertSite alerts and extract timestamps. You can add source types in Splunk web interface, or by editing the `props.conf` file.

Add source type in Splunk web interface

1. Log into Splunk as administrator.
2. Go to the **Source types** configuration screen (for example, **Settings > Source types** in Splunk Enterprise, or menu button > **Data > Source types** in Splunk Light).
3. Click **New Source Type**.
4. Specify the following settings:

Create Source Type

Name: alertsite

Description: optional

Destination app: Search & Reporting

Category: Custom

Indexed Extractions: json

Timestamp

Extraction: Auto

Time zone: (GMT-5:00) America/New_York (E)


Timestamp format: %Y-%m-%d %H:%M:%S

Timestamp fields: details.timestamp,details.tested at,det

Advanced

Name	Value
CHARSET	
SHOULD_LINEMERGE	true
INDEXED_EXTRACTIONS	json
NO_BINARY_CHECK	true
pulldown_type	1
category	Custom
TIME_FORMAT	%Y-%m-%d %H:%M:%S
TZ	America/New_York
TIMESTAMP_FIELDS	details.timestamp,details.tested at,det
KV_MODE	none
AUTO_KV_JSON	false

Cancel Save

Setting	Value
Name	alertsite
Indexed Extractions	json
Timestamp > Extraction	Advanced
Time zone	Select the same time zone as specified in your AlertSite settings in  > Account > AlertSite Preferences > Timezone . For example, if your AlertSite time zone is "GMT-05 Eastern Time (USA)", select the GMT-5 time zone in Splunk too.
Timestamp format	%Y-%m-%d %H:%M:%S
Timestamp fields	details.timestamp,details.tested at,details.fixed at
Advanced	Click New setting and add these settings: KV_MODE = none AUTO_KV_JSON = false

5. Click **Save**.
6. Restart Splunk to complete the configuration.

Add source type via props.conf file

In self-hosted Splunk, you can edit the *props.conf* file in `$SPLUNK_HOME/etc/system/local/` and add the following section:

```
[alertsight]
INDEXED_EXTRactions = json
KV_MODE = none
AUTO_KV_JSON = false
TIMESTAMP_FIELDS = details.timestamp,details.tested at,details.fixed at
```

```
TIME_FORMAT = %Y-%m-%d %H:%M:%S
```

```
TZ = America/New\_York
```

Set **TZ** to the same time zone as specified in your AlertSite settings in  > **Account** > **AlertSite Preferences** > **Timezone**. For possible TZ values, see the [tz database](#).

Restart Splunk to reload the *props.conf* file:

```
splunk restart
```

Tips:

- To receive alerts from specific monitors rather than all monitors, you can create a recipient group containing Splunk and the needed monitors.
- If you use several Splunk servers, you can add them as individual recipients.
- Splunk recipients also appear in your global recipient list in **Alerts** > **Alert Recipients** and you can manage them from there.

New to Splunk?

- Read more about Splunk product offerings here: http://www.splunk.com/en_us/products.html

Questions?

Please contact your customer success advisor if you have any questions. Visit our [document repository](#) to get more information about AlertSite.