# Table of Contents

**Welcome to Splunk Business Flow** ................................................................. 1  
  Welcome to Splunk Business Flow ............................................................... 1  
  SBF concepts and terminology .................................................................. 2  

**Install Splunk Business Flow** ...................................................................... 5  
  Install Splunk Business Flow .................................................................... 5  
  Configure Splunk Business Flow .............................................................. 6  
  Back up and restore your SBF registration information ............................. 8  
  Upgrade Splunk Business Flow ................................................................ 10  
  Share data in Splunk Business Flow ......................................................... 11  
  Splunk Business Flow compatibility matrix ............................................. 13  

**Manage users and roles** .............................................................................. 15  
  Configure roles and manage access to Splunk Business Flow ............... 15
Welcome to Splunk Business Flow

Welcome to Splunk Business Flow

Welcome to Splunk Business Flow (SBF). SBF is a process mining solution that allows users to explore and visualize business processes, discover connections across disparate systems, and optimize flows.

Where to start

To install SBF, see Install Splunk Business Flow.

If you are new to SBF, see the Getting Started Tutorial.

To review the known issues, fixed issues, and new features, see Release Notes for Splunk Business Flow.

To learn more about features and concepts in SBF, see the user manual Splunk Business Flow User Manual.

How to administer Splunk Business Flow for your organization

As Splunk platform administrator, you are responsible for the following Splunk Business Flow administration tasks.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install SBF</td>
<td>You must install the app.</td>
<td>Install Splunk Business Flow</td>
</tr>
<tr>
<td>Configure SBF</td>
<td>You must register the app with the SBF Hosted Environment, add your license, and select a Hosted Environment version.</td>
<td>Set up Splunk Business Flow</td>
</tr>
<tr>
<td>Assign roles and capabilities</td>
<td>You can assign roles and capabilities to your users.</td>
<td>Configure roles and manage access to Splunk Business Flow</td>
</tr>
<tr>
<td>Back up and restore your registration</td>
<td>Backing up your registration information allows you to restore the app on the existing search head or migrate it to a different</td>
<td>Back up and restore your SBF registration</td>
</tr>
</tbody>
</table>
SBF concepts and terminology

The following examples introduce important terminology and concepts in SBF.

Terminology

In SBF you create a Flow Model, define the fields you want to track and correlate, and explore Journeys. Then, save your analyses as a Flow.

Flow Model

"Flow Model" refers to a grouping of discrete information which represents a transaction, session, or other business process that is configured within Splunk Business Flow. The Flow Model contains a repository of events that you are interested in analyzing. In the Flow Model, you define what field names you want to track, and how you want to correlate events. The following components make up a Flow Model definition: a search and the fields that represent one or more Correlation IDs, Steps, and Attributes. The Search scans the event logs, transforms or extracts events based on the specifications of the search, and then returns the results. The Flow Model definition determines how SBF identifies and groups related events into ordered sequences called Journeys.

Flow

A Flow is a saved view of the analyses and settings you applied to the Flow Model in the Explorer. These include step filters, Journey duration, conversion funnels, and metric summaries. You can create multiple Flows from the same Flow Model. All changes to Flow Models propagate to related Flows. Saving your work as a Flow enables users who do not have knowledge of SPL to interact with and explore the data.
**Journey**

A Journey contains all the Steps a user or object executes during a process. For example, suppose you create a Flow Model to analyze order system data for an online clothes retailer. A sample Journey in this Flow Model could track an order from time of placement to delivery.

**Step**

A step is the status of an action or process you want to track. The customer steps for a Journey in the order system Flow model could be: order placed, order shipped, order in transit, order delivered.

**Correlation ID**

Correlation IDs are the field name that correspond to unique descriptors of events such as user_ID, customer_ID, phone_number, or caller_ID. Splunk Business Flow uses Correlation IDs to identify related events and in the event log and group them into Journeys. Continuing with the same example, a Correlation ID for the order system journey would could be the order_id.

**Attribute**

An attribute is an optional component of a Flow Model. An attribute represents additional information you'd like to include in your search, such as location. You can use attributes to filter journeys. For example, you could filter Journeys from the order system Flow Model by the warehouse the item originated from.

**Important terminology and concepts in SBF**

SBF identifies related events and groups them into ordered sequences called Journeys. The following example walks through how SBF groups events into Journeys and Journeys into the Flowchart.

**Event grouping**

In this example, you are interested in tracking how customers make purchases on the Buttercup Game Store website. Consider the event log to be a timeline of events generated from a process or system. Each event contains a timestamp, a step, and a field name which correspond to the Correlation ID.

The Correlation ID in this diagram is user_ID and it corresponds to two field values: user123 and user456. Because there are two distinct identities, there are
two Journeys. Each Journey contains the respective steps the user took during a period of time. The following diagram shows a high level overview of how SBF groups events into Journeys.

### Journey grouping

The Flowchart feature groups a collection of Journeys into a single, ordered sequence of steps. The following diagram represents the Flowchart for the Buttercup Game Store example. This Flowchart contains three Journeys and all of the steps included in those Journeys. The number next to each step reflects the number of Journeys this step appeared in.
Install Splunk Business Flow

Install Splunk Business Flow

Before you install Splunk Business Flow you need to satisfy the following requirements.

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Splunk Enterprise or Splunk Cloud deployment</td>
<td>Splunk Business Flow is an app for the Splunk platform and is compatible with both Splunk Enterprise and Splunk Cloud versions 7.0.x, 7.1.x, 7.2.x, 7.3.x. If you are running an earlier version of Splunk Enterprise, see How to upgrade Splunk Enterprise in the Splunk Enterprise Installation Manual.</td>
</tr>
<tr>
<td>Role</td>
<td>You must be a Splunk platform administrator to install and set up Splunk Business Flow on your Splunk platform deployment.</td>
</tr>
<tr>
<td>Browser</td>
<td>Splunk Business Flow supports the latest versions of Chrome, Firefox, and Internet Explorer 11.</td>
</tr>
<tr>
<td>Internet connectivity</td>
<td>The search head and browser must be connected to the internet to use Splunk Business Flow. To connect the search head to the internet you might need to set up an HTTPS proxy server for Splunkd. To set up an HTTPS proxy server, see Configure Splunk for proxy in the Splunk Enterprise Admin Manual.</td>
</tr>
</tbody>
</table>

Install Splunk Business Flow on a single-instance deployment of Splunk Enterprise

Follow these steps to install Splunk Business Flow on a single-instance Splunk Enterprise deployment.

1. Download the app from Splunkbase using your entitlement account.
2. Untar the downloaded file in the $SPLUNK_HOME/etc/apps directory on *nix or %SPLUNK_HOME%\etc\apps directory on Windows.
3. Restart Splunk Enterprise.
Install Splunk Business Flow in a distributed search deployment

In a distributed deployment, install Splunk Business Flow on your search heads or search head cluster only.

For unclustered search heads, follow the same procedure as a single-instance deployment:

1. Download the app from Splunkbase using your entitlement account.
2. Untar the downloaded file in the $SPLUNK_HOME/etc/apps directory of your search head on *nix or %SPLUNK_HOME%\etc\apps directory of your search head on Windows.
3. Restart the search head.

For a search head cluster, use the configuration bundle method to distribute the app to your cluster members. See Deploy a configuration bundle in the Splunk Enterprise Distributed Search manual.

Install Splunk Business Flow on Splunk Cloud

To request installation of Splunk Business Flow on your Splunk Cloud instance, log a case using the Splunk Support Portal.

Configure Splunk Business Flow

After you install Splunk Business Flow, a Splunk platform administrator must perform the following configuration tasks:

- Register Splunk Business Flow
- Add a license for Splunk Business Flow
- Configure your Hosted Environment version

Register Splunk Business Flow

Follow these steps to register your installation of Splunk Business Flow with the SBF Hosted Environment.

1. Log in to your Splunk platform deployment.
2. Click the Splunk Enterprise home button.
3. Click Splunk Business Flow under apps.
4. On the **Register to use Splunk Business Flow** page, wait for the Health Check to finish confirming that your search head has the required connectivity with the SBF Hosted Environment.

5. Under **Choose the region in which application metadata will reside** select either `us` for United States or `eu` for Europe.

6. Select the license you want to apply.
   1. Add a license and enter the license GUID.
   2. Use the 30 Day Trial Version.

- Click **Register**.

**Add and manage licenses for Splunk Business Flow**

Follow these steps to add the license key for Splunk Business Flow:

1. Click the gear icon to open the Configuration page.
2. Click the **Licensing** tab.
3. Click **Add License**.
4. Enter your License GUID.
5. Click **Add**.

To delete a license, click **Delete** under Actions.

**Configure your Hosted Environment version**

The Splunk Business Flow app offers two versions of the SBF Hosted Environment: Stable and Latest.

If you choose the Latest version, your user experience is updated with most recent version of the SBF Hosted Environment as soon as the product team makes changes. Updates to the Latest version can occur frequently.

If you choose the Stable version, your user experience remains consistent over longer periods. Approximately three times a year, the Stable version receives a batched update of the changes that have accrued in the Latest version since the last change to Stable.

To switch your Hosted Environment version, follow these steps:

1. Click the gear icon to open the Configuration page.
2. Click the **Release Management** tab.
3. Click the radio button next to **Stable** or **Latest**.
4. Click **Update and Reload**.
Back up and restore your SBF registration information

After you install the Splunk Business Flow (SBF) app, you can generate a ZIP file to back up the SBF registration information.

Why backup your Registration information?

Backing up your registration information allows you to restore the app on the existing search head or migrate it to a different search head. Suppose you have more than one search head in your deployment. For example, as a Splunk administrator, you might want to try out the SBF app on one search head before migrating it to another search head with more users.

What's in the backup file?

The backup file sbf_backup.zip contains your SBF registration information: the tenant ID, registration ID, PEM files, PEM password, and the SBF production environment URL. The backup file does not contain any event data or Flow Model definitions. The registration data includes a public and private key pair that is used to authenticate and encrypt the server-to-server communication between your Splunk search head and the Splunk Business Flow Hosted Environment.

What happens when you back up and restore your SBF registration information on a search head cluster

The following example outlines what happens when you back up and restore your SBF registration information on a search head cluster. If you use a Deployer, you might not need to install SBF on more than one search head. To see if this applies to you, see Use the deployer to distribute apps and configuration updates in the Splunk Enterprise Distributed Search Manual.

Suppose you are a business analyst at the fictitious Buttercup Games company. Your company's Splunk deployment has two search head clusters, one for development and one for production. Each cluster contains three search heads. You have installed the app on one search head in the development cluster and backed up your SBF registration information. In the production cluster, SBF is installed on two search heads.

After trying out the app on the development search head, you decide to migrate the SBF app to the production search head cluster. You install the SBF app on
two search heads in the production cluster. You need to restore your registration information on only one search head in the production cluster. After you perform the restore, both installations of the SBF app in the production cluster contain your SBF registration information.

The following diagram illustrates a high-level overview of your Splunk deployment and the back up restore process at Buttercup Games.

Back up your registration information

Generate the `sbf_backup.zip` file to back up your registration information.

**Prerequisites** Set the `$SPLUNK_HOME` environment variable if it hasn’t been set already. To check if the environment variable is set up and to set the path, see Set `$SPLUNK_HOME` in the Splunk Dev portal.

Store the backup file securely because it contains sensitive information.

**Steps**

1. In the command line, enter the following with your file path `<YOUR_ZIP_PATH>`:
   ```
   $SPLUNK_HOME/bin/splunk cmd python
   $SPLUNK_HOME/etc/apps/splunk-business-flow/sbf_backup.py backup <YOUR_ZIP_PATH>
   ```
2. Confirm the Splunk admin REST URL `localhost:8089`
3. Enter your Splunk admin username and password.
   The script returns the path of the backup file `sbf_backup.zip`.

**Restore your SBF registration information**

After you generate the `sbf_backup.zip` you can restore your SBF registration information on the same search head or migrate it to a different search head.
Steps:

1. (Optional) Copy the `sbf_backup.zip` file path to the desired directory to migrate your SBF registration information to a different Splunk search head than where you originally registered it.
2. In the command line, enter the following with your file path `<YOUR_ZIP_PATH>`:
   ```bash
   $SPLUNK_HOME/bin/splunk cmd python
   $SPLUNK_HOME/etc/apps/splunk-business-flow/sbf_backup.py restore
   <YOUR_ZIP_PATH>
   ```
3. Enter your Splunk admin username and password.
   If the reset is successful the script returns the following statement: Done performing restore.

Upgrade Splunk Business Flow

When a new release of Splunk Business Flow is available, you can upgrade the app two different ways: in Splunk Web or from Splunkbase.

Upgrade the app in Splunk Web

When the application has an upgrade available a notification appears in the Splunk messages list.

1. In the upgrade notification message, click **Update**.
2. Click **Accept and Continue**.
3. Enter your Splunk.com log in credentials.
4. Click **Login and Continue**.
5. Click **Restart Now**.

Upgrade the app from Splunkbase

You can also upgrade the app through Splunkbase.

1. Go to https://splunkbase.splunk.com
2. Enter Splunk Business Flow in the search bar.
3. Download the latest version of the app.
4. Log in to your Splunk platform deployment.
5. In Splunk Web, click the Apps gear icon.
6. Click **Install app from file**.
7. Click **Choose File**.
8. Select the file and click **Open**.
9. Check the **Upgrade app** box.
10. Click **Upload**.

## Share data in Splunk Business Flow

When Splunk Business Flow is deployed on Splunk Enterprise, the Splunk platform sends anonymized usage data to Splunk Inc. ("Splunk") to help improve Splunk Business Flow in future releases. For information about how the data is collected, stored, and governed, see Share data in Splunk Enterprise.

### What data is collected


**Splunk Business Flow Hosted Environment telemetry**

Splunk Business Flow may collect telemetry about the SBF Hosted Environment, including data like:

- Anonymized user interactions with features in the application's user interface
- Latency and other performance statistics for operations and user actions
- API interactions with server components in the SBF Hosted Environment

Telemetry data about the Splunk Business Flow Hosted Environment is collected automatically, regardless of the opt-in or opt-out decision you make for Splunk platform telemetry.

### App usage information

Splunk Business Flow collects the following usage information about the app:

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>app.session.tokenLoadError</td>
<td>Tracks authentication token loading errors.</td>
</tr>
</tbody>
</table>

{ "error": "Error connecting to server. Check "https://eu.businessflowapp.splunk.com/60b46b9d-c922-46f2-a816-2db3375484ff." }
<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>app.session.tokenLoadSuccess</td>
<td>Tracks authentication token success.</td>
</tr>
<tr>
<td>{</td>
<td></td>
</tr>
<tr>
<td>tenantId&quot;: &quot;4376dc04-99fe-496c-9924-f3143e975b55&quot;,</td>
<td></td>
</tr>
<tr>
<td>target&quot;: &quot;<a href="https://eu.businessflowapp.splunk.com">https://eu.businessflowapp.splunk.com</a>&quot;,</td>
<td></td>
</tr>
<tr>
<td>page&quot;: &quot;explore&quot;,</td>
<td></td>
</tr>
<tr>
<td>app&quot;: &quot;splunk-business-flow&quot;</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td></td>
</tr>
<tr>
<td>app.session.appInitError</td>
<td>Tracks errors initializing the application or connecting with the SBF Hosted Environment.</td>
</tr>
<tr>
<td>{</td>
<td></td>
</tr>
<tr>
<td>error&quot;: &quot;Failed to update cloud server: 72c90bb4-c537-46de-a28e-1acdac47870c. &quot;</td>
<td></td>
</tr>
<tr>
<td>page&quot;: &quot;home&quot;,</td>
<td></td>
</tr>
<tr>
<td>app&quot;: &quot;splunk-business-flow&quot;</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td></td>
</tr>
<tr>
<td>app.session.uncaughtJsError</td>
<td>Tracks uncaught JavaScript errors in the browser.</td>
</tr>
<tr>
<td>{</td>
<td></td>
</tr>
<tr>
<td>app&quot;: &quot;splunk-business-flow&quot;,</td>
<td></td>
</tr>
<tr>
<td>error&quot;: &quot;Uncaught Error: ajax error&quot;,</td>
<td></td>
</tr>
<tr>
<td>handler&quot;: &quot;on-prem UI window error handler&quot;,</td>
<td></td>
</tr>
<tr>
<td>page&quot;: &quot;setup&quot;</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td></td>
</tr>
<tr>
<td>Component</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| app.session.acceptAgreementError | Tracks errors processing acceptance of the user agreement.                   | { "error": "Something went wrong. X-Request-ID: 72c90bb4-c537-46de-a28e-1acdac47870c.
  "page": "home",
  "app": "splunk-business-flow" } |
| app.session.registrationError   | Tracks errors registering with the SBF Hosted Environment.                   | { "error": "Error with decrypt: Error with OpenSSL RSA decrypt: 1. X-Request-ID: cc4a0b03-e904-4ff3-bfd3-79da8c7e5a34.
  "page": "home",
  "app": "splunk-business-flow" } |
| app.session.loadRegistrationError | Tracks errors loading information about an existing registration with the SBF Hosted Environment. | { "error": "Something went wrong. X-Request-ID: 72c90bb4-c537-46de-a28e-1acdac47870c.
  "page": "home",
  "app": "splunk-business-flow" } |

**Splunk Business Flow compatibility matrix**

The SBF package versions are compatible and supported by the following Splunk Enterprise and Splunk Cloud versions for the given time period. For the support status of these Splunk products, see the Splunk Software Support Policy.

<table>
<thead>
<tr>
<th>SBF package number</th>
<th>Splunk Enterprise version</th>
<th>Splunk Cloud version</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0.2</td>
<td>Splunk Enterprise 7.0.x, 7.1.x, 7.2.x, 7.3.x</td>
<td>Splunk Cloud version 7.0.x, 7.1.x, 7.2.x, 7.3.x</td>
</tr>
<tr>
<td>SBF package number</td>
<td>Splunk Enterprise version</td>
<td>Splunk Cloud version</td>
</tr>
<tr>
<td>--------------------</td>
<td>--------------------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>19, 2019</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.0.1 Released May, 16, 2019</td>
<td>Splunk Enterprise 7.0.x, 7.1.x, 7.2.x, 7.3.x</td>
<td>Splunk Cloud version 7.0.x, 7.1.x, 7.2.x, 7.3.x</td>
</tr>
<tr>
<td>1.0.0 Released April, 29, 2019</td>
<td>Splunk Enterprise 7.0.x, 7.1.x, 7.2.x, 7.3.x</td>
<td>Splunk Cloud version 7.0.x, 7.1.x, 7.2.x, 7.3.x</td>
</tr>
</tbody>
</table>
Manage users and roles

Configure roles and manage access to Splunk Business Flow

To manage role-based access in Splunk Business Flow (SBF), use the access control system built into the Splunk platform for authentication and authorization. Splunk platform administrators use this access control system to add users, assign users to roles, and assign those roles custom capabilities to provide limited, role-based access control for your organization.

Splunk Business Flow adds one role to the default roles provided by the Splunk platform. This role is unique to SBF and does not apply to Splunk Enterprise or other Splunk apps.

sbf_modeler

Assign this role to SBF users with strong domain expertise who are business process experts. This role inherits all the capabilities of the power role and also provides the sbf_set_visibility_flow_model and sbf_edit_flow_model capabilities. Private Flow Models may only be used by the administrative Splunk Business Flow Modeler role for testing, configuration and preview of Flow Models.

As a Splunk platform administrator, you can assign users to this role. For more about assigning roles, see Add and edit roles in Splunk Web in Securing Splunk Enterprise.

Capabilities inherited from Splunk platform roles

The sbf_modeler role inherits capabilities from the Splunk platform power role.

<table>
<thead>
<tr>
<th>SBF role</th>
<th>Inherited Splunk platform role</th>
<th>Added capabilities in SBF</th>
<th>Can be assigned</th>
<th>Package version</th>
</tr>
</thead>
<tbody>
<tr>
<td>sbf_modeler</td>
<td>power</td>
<td>sbf_set_visibility_flow_model, sbf_edit_flow_model</td>
<td>Yes</td>
<td>1.0.0</td>
</tr>
</tbody>
</table>
## Capabilities in SBF

SBF includes the following capabilities.

<table>
<thead>
<tr>
<th>Capability</th>
<th>Description</th>
<th>sbf_modeler</th>
<th>admin</th>
<th>Package version</th>
<th>Application version</th>
</tr>
</thead>
<tbody>
<tr>
<td>sbf_set_visibility_flow_model</td>
<td>Ability to set a Flow Model to Private or Shared.</td>
<td>X</td>
<td>X</td>
<td>1.0.0</td>
<td>Stable, Latest</td>
</tr>
<tr>
<td>sbf_set_app_version</td>
<td>Ability to set the app to Stable or Latest and the reverse.</td>
<td>X</td>
<td></td>
<td>1.0.0</td>
<td>Stable, Latest</td>
</tr>
<tr>
<td>sbf_edit_flow_models</td>
<td>Ability to create, edit, clone, and delete a Flow Model. Flow Models are inaccessible to all users who do not have the sbf_edit_flow_models capability.</td>
<td>X</td>
<td>X</td>
<td>1.1.0</td>
<td>Latest</td>
</tr>
</tbody>
</table>