# Table of Contents

## What Is Splunk Cloud?
- Welcome to Splunk Cloud...............................................................1
- Types of Splunk Cloud deployment................................................6
- Getting started with Splunk Cloud...............................................7
- Splunk Cloud Quick Start.............................................................8

## Get data into Splunk Cloud
- Overview of getting data into Splunk Cloud.................................12
- Forward data to Splunk Cloud from Microsoft Windows..............15
- Forward data to Splunk Cloud from Linux..................................19
- Forward data to Splunk Cloud from MacOS...............................22
- Forward data from files and directories to Splunk Cloud.............26

## Administer Splunk Cloud
- Overview of Splunk Cloud administration..................................29
- Splunk Cloud data policies.........................................................30
- Monitor Splunk Cloud deployment health..................................32
- Manage Splunk Cloud indexes......................................................44
- Store expired Splunk Cloud data...............................................49
- Archive expired Splunk Cloud data..............................................58
- Manage Splunk Cloud users and roles.......................................64
- Configure SAML single sign-on (SSO) to Splunk Cloud.............69
- Configure hybrid search..............................................................69
- Install apps in your Splunk Cloud deployment..........................71
- Manage private apps in your Splunk Cloud deployment..............73
- Manage a rolling restart in Splunk Cloud..................................77
- Upgrade your Forwarders.........................................................78
What Is Splunk Cloud?

Welcome to Splunk Cloud!

This manual contains information to help you get your data into Splunk Cloud, create reports and dashboards, and work with Splunk Support to administer Splunk Cloud and get help.

Splunk Cloud enables you to store, search, analyze, and visualize the machine-generated data gathered from the websites, applications, sensors, devices, and so on, that comprise your IT infrastructure or business. Splunk Cloud offers many of the features of Splunk Enterprise as a cloud service. You can use Splunk Cloud alone or with Splunk Enterprise on-premises software as a hybrid solution. Splunk Cloud deployments are continuously monitored and managed by the Splunk Cloud Operations team.

To send data to Splunk Cloud, you run **forwarders** on machines that have access to the source data. Splunk Cloud software ingests the forwarded data and **indexes** it, transforming it into searchable knowledge in the form of **events**. After **event processing** is complete, you can associate events with **knowledge objects** to enhance their usefulness. For example, you can use the search processing language or the interactive pivot feature to create reports and visualizations.

The Splunk Cloud Service

When you subscribe to the Splunk Cloud service, you get a dedicated Splunk deployment that is hosted in Amazon Web Services. Splunk Cloud is available in the following Amazon Web Services (AWS) regions: US (Virginia, Oregon, GovCloud), EU (Dublin, Frankfurt, London), Asia Pacific (Singapore, Sydney, Tokyo) and Canada (Central). For details, contact your sales representative or email sales@splunk.com before purchasing.

Features of the Splunk platform

The following table lists major features of the Splunk platform. For detailed information, refer to Splunk.com and Splunk Docs.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Indexing</td>
<td></td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Splunk</td>
<td>Splunk software indexes machine data. This includes data from packaged and custom applications, application servers, web servers, databases, networks, virtual machines, telecoms equipment, operating systems, sensors, and so on, that make up your IT infrastructure. (More information)</td>
</tr>
<tr>
<td>Data model</td>
<td>A data model is a hierarchically-structured search-time mapping of semantic knowledge about one or more datasets. It encodes the domain knowledge necessary to build a variety of specialized searches of those datasets. These specialized searches are used to generate reports for Pivot users. Data model objects represent different datasets within the larger set of indexed data. (More information)</td>
</tr>
<tr>
<td>Pivot</td>
<td>Pivot refers to the table, chart, or data visualization you create using the Pivot Editor. The Pivot Editor lets users map attributes defined by data model objects to a table or chart data visualization without having to write the searches to generate them. Pivots can be saved as reports and added to dashboards. (More information)</td>
</tr>
<tr>
<td>Search</td>
<td>Search is the primary way that you navigate data that you have stored in your Splunk deployment. You can write a search to retrieve events from an index, use statistical commands to calculate metrics and generate reports, search for specific conditions within a rolling time window, identify patterns in your data, predict future trends, and so on. You can save searches as reports and use them to power dashboard panels. (More information)</td>
</tr>
<tr>
<td>Alerts</td>
<td>Alerts are triggered when conditions are met by search results for both historical and real-time searches. Alerts can be configured to trigger actions such as sending alert information to designated email addresses, posting alert information to an RSS feed, or running a custom script, such as one that posts an alert event to syslog. (More information)</td>
</tr>
<tr>
<td>Reports</td>
<td>Reports are saved searches and pivots. You can run reports on an ad hoc basis, schedule them to run on a regular interval, or set scheduled reports to generate alerts when the results of their runs meet particular conditions. You can add reports to dashboards as dashboard panels. (More information)</td>
</tr>
<tr>
<td>Dashboards</td>
<td>Dashboards are made up of panels that contain modules such as search boxes, fields, charts, tables, forms, and so on.</td>
</tr>
</tbody>
</table>
Dashboard panels are usually hooked up to saved searches or pivots. They can display the results of completed searches as well as data from backgrounded real-time searches. (More information)

### Differences between Splunk Cloud and Splunk Enterprise

Splunk Cloud provides a layer of security and operational control that causes it to differ from Splunk Enterprise, as follows:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Splunk Enterprise</th>
<th>Splunk Cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command line interface</td>
<td>Available</td>
<td>Splunk Cloud customers do not have access to the command line. You can perform many administrative tasks through the web browser, such as managing indexes and source types. Other tasks that require CLI access must be performed on your behalf by Splunk Support.</td>
</tr>
<tr>
<td>Apps</td>
<td>You decide what apps run in your deployment</td>
<td>Only apps that have been evaluated for security and stability and approved by Splunk are permitted to run in Splunk Cloud. You can use Splunk Web to install vetted apps.</td>
</tr>
<tr>
<td>Direct TCP and syslog inputs</td>
<td>Supported</td>
<td>You cannot send these types of data directly to Splunk Cloud. You must use an on-premises forwarder to send such data.</td>
</tr>
<tr>
<td>Scripted alerts</td>
<td>Supported</td>
<td>Supported only in the context of approved apps</td>
</tr>
<tr>
<td>License pooling</td>
<td>Supported</td>
<td>Not supported. The license manager is not Internet-accessible to Splunk Cloud customers.</td>
</tr>
<tr>
<td>HTTP event collector (HEC)</td>
<td>Enabled by default</td>
<td>For managed Splunk Cloud deployments, HEC must be enabled by Splunk Support and uses port 443 (Splunk Enterprise uses port 8088).</td>
</tr>
<tr>
<td>Splunk API</td>
<td>Enabled by default</td>
<td>Disabled by default for managed Splunk Cloud deployments. Contact Splunk Support to enable access for managed Splunk Cloud deployments, Splunk Cloud trials, and sandboxes.</td>
</tr>
</tbody>
</table>
Get help with Splunk Cloud

To learn more about Splunk features, see the manuals on the Splunk docs web site. To find other Splunk users near you, see the Splunk user group web site. To learn about how other organizations are succeeding with Splunk Cloud, watch On The Road with AAA and Splunk Cloud.

Splunk Technical Support

As a Splunk Cloud customer, you can rely on Splunk Support to administer and optimize Splunk Cloud for you. Contact Support in the following ways.

- On the Web: Submit an issue.
- By telephone: Call us
- Learn more about Splunk Support programs

Contact Splunk Support to:

- Obtain REST API credentials
- Reset a user password
- Link to an LDAP directory
- Modify the configuration settings of your deployment
- Report an outage,
- Report an issue
- Request a feature or change to your deployment.

For details about the levels of technical support provided, read Support Programs. Only authorized support contacts from your company can open cases. Your Splunk support agreement specifies who your authorized contacts are. Your Support contract specifies a number of authorized contacts, and an expiration date. One of your contacts is a Support portal administrator, who can update the list. Only an authorized contact can open a case and track its status.

An authorized contact can file a case in one of two ways:

- Log in to splunk.com and navigate to the Support Portal.
- In Splunk Cloud, click About and select File a Bug.

Splunk Support portal

Designated Splunk Cloud users can manage operational contacts for their account and file support cases using the Support portal. Operational contacts are the people in your organization who are notified when their Splunk Cloud
environment undergoes maintenance or experiences an event that affects performance.

**To manage operational contacts:**

2. Follow the instructions on the page to add, edit, and remove operational contacts for your Splunk Cloud environment.

**To file a case on the Support portal:**

1. From the **Splunk installation is?** dropdown, select the state of your deployment.
2. In **Subject**, summarize your issue. Splunk Support sees the first 250 characters in this field.
3. In **What Product are you having trouble with?** select **Splunk Cloud**.
4. In **What OS are you using?** select **Linux**.
5. Leave **What OS Version are you using?** blank.
6. In **I need help with...** select a category that applies to your issue.
7. In **What is the impact...** explain briefly how this issue disrupts your work.
8. In the **Problem Description**, be thorough. For issues (as opposed to enhancement requests), include the exact time of the issue and its duration, the type of Splunk instance experiencing the issue (for example, forwarder, search head, or indexers), and any relevant screen shots.
9. Include **Steps to reproduce** if you've found a specific scenario that triggers the issue.
10. Click **Submit**. The portal directs you to a screen with a case number and sends you an email containing the case number.

Splunk Support replies to the case creator by email. You can update the case by replying to the email (be sure to keep the tracking ID in the email subject line). You can also update the case, check on its status, or close a case using the support portal.

**Splunk community**

The Splunk user community is a great resource. Check out Splunk Answers, where you can ask and answer questions about the product, or chat live with community members in our IRC channel.
Types of Splunk Cloud deployment

Splunk Cloud is offered in two ways:

- **Self-service**: You purchase Splunk Cloud directly from the Splunk website.
- **Managed**: You work with Splunk Sales to obtain your Splunk Cloud deployment.

To determine whether your deployment is self-service or managed, look at the format of the URL you use to connect to Splunk Cloud:

- **Self-service**: https://prd-*.cloud.splunk.com
- **Managed**: https://*.splunkcloud.com

The following table lists details about the differences between managed and self-service deployments.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Self-service</th>
<th>Managed</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Access your Splunk Cloud deployment</strong></td>
<td>Log into your Splunk account on the Splunk corporate web site (<a href="http://www.splunk.com">www.splunk.com</a>) and go to the <strong>Access Instances</strong> page</td>
<td>Using the URL you specified when you purchased Splunk Cloud from Splunk Sales. This URL is included in the Welcome email you received when your deployment was enabled for you.</td>
</tr>
<tr>
<td><strong>Create inputs</strong> (including file uploads, HTML event ingestion, and app-related inputs)</td>
<td>Configure forwarders on-premises or use Splunk Web</td>
<td>Configure forwarders on-premises or contact Splunk Support</td>
</tr>
<tr>
<td><strong>Data ingestion</strong> (daily maximum)</td>
<td>20GB</td>
<td>Per your contract</td>
</tr>
<tr>
<td><strong>Active Directory/Single sign-on integration</strong></td>
<td>Not supported</td>
<td>Supported</td>
</tr>
<tr>
<td><strong>AWS regions</strong></td>
<td>US East</td>
<td>Multiple including GovCloud</td>
</tr>
<tr>
<td><strong>Whitelist and blacklist IP addresses</strong></td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Feature</td>
<td>Self-service</td>
<td></td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Premium apps available</td>
<td>Yes, but you might need to add capacity to your Splunk Cloud deployment, which entails additional costs. (<em>&quot;Premium&quot; apps and add-ons are purchased from Splunk Sales, as opposed to free apps, which you can install without contacting Splunk Sales or Support.</em>)</td>
<td>Yes</td>
</tr>
<tr>
<td>Concurrent search limit</td>
<td>20 max&lt;br&gt;Depends on the topology you purchase</td>
<td></td>
</tr>
<tr>
<td>REST API URL</td>
<td>Use the following URL for self-service deployments. To get the required non-SAML user credentials, submit a support case. The URL format must include the &quot;input-&quot; prefix:&lt;br&gt;<a href="http://input-">http://input-</a>&lt;deployment-name&gt;.cloud.splunk.com:8089&lt;br&gt;Use the following URL for clustered deployments. If necessary, submit a support case to open port 8089 on your deployment. The &quot;input-&quot; prefix is not required:&lt;br&gt;https://&lt;deployment-name&gt;.splunkcloud.com:8089</td>
<td></td>
</tr>
</tbody>
</table>

### Getting started with Splunk Cloud

To start using your new Splunk Cloud deployment, you or your Splunk administrator need to:

- Log in
- Get data in
- Create reports based on your data

### Log into Splunk Cloud

If you bought self-service Splunk Cloud directly on the Splunk web site, you received a cloud.splunk.com URL and credentials. If you worked with Splunk Sales to purchase managed Splunk Cloud, you received an email with a dedicated URL and login credentials as part of the purchase process.

1. Open your web browser.
2. Navigate to your Splunk Cloud URL.
3. Log in using the credentials supplied by Splunk Sales or Support.

### Get data into Splunk Cloud

To get data into Splunk Cloud, the most common approach is to install the Splunk Universal Forwarder and required credentials on the computers where your source data resides and configure them to send data to Splunk Cloud. For details about the options for getting data into Splunk Cloud, see Overview of
getting data into Splunk Cloud.

**Search and render your data**

After you get your data into Splunk Cloud, you can search the data to create reports and display the results using dashboards and visualizations. For detailed information, see the following manuals.

- Search Manual
- Reporting Manual
- Dashboards and visualizations

**Learn about Splunk products**

For detailed information about the Splunk platform, see the following resources.

- Splunk Docs is Splunk user documentation.
- Splunk Answers is our thriving user community. Join us!
- Splunk Education offers courses on-site, off-site, and on the Web.
  - Splunk Tutorial (free)
  - Building Add-ons (free)
  - Using Splunk
  - Searching & Reporting with Splunk
  - Creating Splunk Knowledge Objects
  - Splunk Cloud Administration
- Splunk Videos offer training and demos on a variety of topics.

Apps and add-ons extend the power of Splunk products to help you get value from your data faster. To browse Splunk apps and add-ons, see Splunkbase. If you develop your own app, read Splunk Developer Guidance. For an example of a properly constructed app, see the Splunk Reference App.

**Splunk Cloud Quick Start**

If you are new to Splunk Cloud and want to get started quickly, the following steps tell you how to get some data into your Splunk Cloud deployment and search it.
What you need

- Your Splunk Cloud URL, Splunk username, and password. When you bought Splunk Cloud, you received an email containing this information, to enable you to log in to your Splunk Cloud deployment. If you have self-service Splunk Cloud, it’s the username and password that you use to log into www.splunk.com.
- A standard type of log file that resides on your computer to use as sample data for this exercise, like a /var/log/messages file on a Unix machine, or a text file in C:\Windows\System32\LogFiles on a Windows computer.

Step 1. Log into Splunk Cloud

1. Open your web browser.
2. Navigate to your Splunk Cloud URL. (Examples: https://mycompany.splunkcloud.com or https://prd-p-njqlk23gjdh.cloud.splunk.com)
3. Log in using the credentials supplied by Splunk Sales or Support.

You are now viewing Splunk Web, the browser-based GUI where you work with your Splunk Cloud deployment.

Step 2. Upload a file

In Splunk Web, perform the following steps:

1. To create a test index where you can store test data, choose Settings > Indexes.
2. On the Indexes page, click New Indexes and assign the index a name. To minimize resource consumption, specify a small size and retention period.
3. Select Settings from the menu bar and click Add Data.
4. On the **Add Data** page, click **Upload**.
5. Click the **Select File** button, browse to a log file on your computer, and click **Choose**. The file is uploaded.
6. Click the **Next** button.
7. On the **Set Source Type** screen, choose the correct source type for the file you uploaded, or, if none is appropriate, specify a name for the new source type and click **Next**.
8. On the **Input Settings** page, choose your test index.
9. Click **Review** and verify your settings.
10. Click **Submit**.

After your data is uploaded, Splunk Web displays a "Success" message. Your data is now ready for you to search.

**Step 3. Search your data**

From the "Success" screen, click the **Start searching** button. Splunk Web displays the data from the log file that you just uploaded, parsed into time-stamped events. If you do not see search results, verify that the time range displayed to the right of the search bar corresponds to the time range of the events in the file that you uploaded.

![New Search](image)

**Step 4. Forward data**

To feed data continually to your Splunk Cloud deployment, you install and configure the Splunk **universal forwarder** on the machine where the data resides. For details about installing and configuring forwarders, refer to the platform-specific documentation below:

- Forward data to Splunk Cloud from Microsoft Windows
- Forward data to Splunk Cloud from Linux
- Forward data to Splunk Cloud from Macintosh OS X

As with the data you uploaded, you can isolate your test data from any production data by forwarding it to a test index.
Next steps

- Send data directly to your Splunk Cloud deployment using HTTP protocol. For details, see Set up and use HTTP Event Collector.

- Create users and administer their access to your Splunk Cloud deployment. For details, see Manage Splunk Cloud users.
Get data into Splunk Cloud

Overview of getting data into Splunk Cloud

This topic provides an overview of the methods available to you for adding data to your Splunk Cloud deployment. For detailed information about what Splunk Cloud can index, see the *Getting Data In* manual.

Type of data that Splunk Cloud accepts

Splunk Cloud accepts a wide variety of data, including IT streaming, machine, and historical data such as Windows event logs, web server logs, live application logs, network feeds, system metrics, change monitoring, message queues, and archive files. Splunk Cloud can monitor relational databases and third-party infrastructures such as DB2, Cisco, Active Directory, Hadoop, and so on.

Splunk Cloud can monitor Windows-specific inputs such as the following:

- Windows Event Log
- Windows Registry
- WMI data
- Active Directory data
- Performance monitoring data

Splunk Cloud can monitor other kinds of data sources. For example:

- First-in, first-out (FIFO) queues
- Scripted inputs
- Modular inputs

Splunk offers apps and add-ons, with pre-configured inputs for specific types of data sources, such as Cisco security data and Blue Coat data.

Options for getting data into Splunk Cloud

You can get data into your Splunk Cloud deployment as follows:

- Forward data from data sources
- Install Splunk apps and add-ons
- Send data using HTTP protocol
**Forward data**

Splunk **forwarders** send data from a datasource to your Splunk Cloud deployment for indexing, which makes the data searchable. Forwarders are lightweight processes, so they can usually run on the machines where the data originates. To forward data to Splunk Cloud, you typically use the Splunk **universal forwarder**.

For forwarder installation instructions, see the topic for your data source platform:

- Microsoft Windows
- Linux
- MacOS

The following diagram illustrates the topology of forwarding data from your corporate network to Splunk Cloud using the universal forwarder.
If you need to anonymize or otherwise preprocess data before it exits your enterprise network, or if a specific app or add-on that you are using does not support universal forwarders, use a **heavy forwarder**. For more information about heavy forwarders, see the Splunk *Forwarding Data* manual.

**Note:** By default, the universal forwarder can forward a maximum of 256 KB of data per second. As a best practice, do not exceed this limit. For more information, read Possible throughput limits in the Splunk Enterprise *Troubleshooting Manual.*

**Use apps to get data in**

Splunk **apps** and **add-ons** extend the capability and simplify the process of getting data into your Splunk platform deployment.

Apps typically target specific data types and handle everything from configuring the inputs to generating useful views of the data. For example, the Splunk App for Windows Infrastructure provides data inputs, searches, reports, alerts, and dashboards for Windows host management. The Splunk App for Unix and Linux offers the same for Unix and Linux environments. There is a wide range of apps to handle specific types of application data, including the following:

- Splunk DB Connect
- Splunk Stream
- Splunk Add-on for Amazon Web Services

Apps and add-ons that contain a data collection component should be installed on forwarders for their data collection functions. See Install apps in your Splunk Cloud deployment.

**Add data using HTTP protocol**

To send HTTP events to Splunk Cloud, you can use the Splunk Java, JavaScript (Node.js), and .NET logging libraries, which are compatible with popular logging frameworks. For test and development purposes, you can use an HTTP client such as the curl utility to send events encoded in JSON.

In addition, you can send data directly to Splunk Cloud using HTTP or HTTPS. To ensure that your credentials are never transmitted from your on-premises systems to Splunk Cloud, this feature uses token-based authentication. For a detailed discussion of the HTTP Event Collector, see the Introduction to Splunk HTTP Event Collector on the Splunk Developer Portal.
If you have a self-service Splunk Cloud deployment (including Splunk Light Cloud Service), use the following format for the URL that you use to access the HTTP event collector:

https://input-prd-p-XXXXXXXX.cloud.splunk.com:8088/services/collector/event,
where XXXXXXX represents the ID assigned to your deployment.

To use the HTTP event collector or an app that relies on it (like Splunk App for Akamai) with a managed Splunk Cloud deployment, create a Splunk Support ticket requesting HTTP event collection to be enabled. Provide the following information:

- Name for data input
- Name for target index
- Source type to be applied to the data
- Amount of data per day that you expect to receive, and any details about your intended usage that will help Splunk Support estimate the number of HTTP connections per hour

In return, Splunk Support sends you the authorization token that is required to send HTTP events to Splunk Cloud.

### Forward data to Splunk Cloud from Microsoft Windows

To get data into Splunk Cloud, log into your Splunk Cloud deployment and do the following:

1. Download the Splunk Universal Forwarder for Windows.
2. Install the Splunk Universal Forwarder for Windows.
3. Download and install the universal forwarder credentials.
4. Configure data inputs, which specify the data to be collected and forwarded.

The following detailed procedure tells you how to install and configure the universal forwarder on a Windows machine.

### Log into your Splunk Cloud deployment

The way you log in depends on whether your Splunk Cloud deployment is managed or self-service (for details, see Types of Splunk Cloud Deployment.)
**Logging into a self-service Splunk Cloud deployment**

1. In your web browser, go to www.splunk.com.
2. Click **My Account**.
3. Click **Log In**.
4. On the **Log In** page, enter the user name and password provided in your "Welcome" email.
5. Choose **My Account > Instances** and click **Access Instance**. The Splunk Cloud user interface displays.

**Logging into a managed Splunk Cloud deployment**

1. In your web browser, go to the URL specified for your deployment. (Your company selected this URL as part of the process of buying Splunk Cloud.)
2. Enter the username and password specified in your Welcome email or provided to you by your Splunk administrator.

**Step 1: Download the installer**

From the Splunk Cloud Home page:

1. In the left sidebar, click **Universal Forwarder**.
2. On the splunkclouduf Home page, click **Download Universal Forwarder**.
3. On the **Download Splunk Universal Forwarder** page, click **Windows** and choose your Windows platform.
4. When prompted, click **Save File** and click **OK** to download the `splunkforwarder` installer, which is an .msi file.

By default, the installer file is saved to the \Users\Downloads directory. If you download it to a different directory, make a note of the location.

**Step 2: Install the universal forwarder**

Install the universal forwarder on the computer that contains or has access to the data that you want to collect and forward to Splunk Cloud. If you want to install the universal forwarder on a different computer, copy the universal forwarder package file to that machine and continue with the steps below.

1. To launch and run the installer, double-click the installer file that you downloaded.
2. When prompted, read the license agreement and select **Check this box to accept the License Agreement**.
3. Uncheck the checkbox labeled **Use this Universal Forwarder with on-premises Splunk Enterprise. Uncheck if you want this Universal Forwarder to contact a Splunk Cloud instance.**

4. Click **Next**.

5. **(Self-service Splunk Cloud deployments only)** To enable you to use Splunk Web to manage forwarders and configure data inputs) In the **Deployment Server** dialog, enter your Splunk Cloud hostname in the **Hostname or IP field**. Specify the URL provided in your Welcome email, omitting the leading `https://` and preceding the URL with "input-". For example: `input-prd-p-z41nh2qlt7cx.cloud.splunk.com`. **(Note: When you install the universal forwarder on other platforms, you must configure the deployment server/client settings manually by editing .conf files. On Windows, this logic is included in the installer.)**

6. For port number, enter **8089**.

7. Click **Next**.

8. Click **Install** to launch the Setup Wizard and begin the installation. **Note:** By default, the **Splunk Universal Forwarder** is installed in the **Program Files** directory. If you install it in another directory, make note of the location.

9. Click **Finish** when prompted.

**Step 3: Download and install the universal forwarder credentials**

To enable the forwarder to send data to Splunk Cloud, you must download the universal forwarder credentials file, which contains a custom certificate for your Splunk Cloud deployment. The universal forwarder credentials are different from the credentials that you use to log into Splunk Cloud.

When you install the credentials file into the universal forwarder, note that the default username and password for a first-time installation of the universal forwarder is `admin:changeme`. To change the admin password, run the `edit user` command. For example: `splunk edit user admin -password mynewpassword -auth admin:changeme`

To install your universal forwarder credentials from the Splunk Cloud Home page:

1. In the left sidebar, click **Universal Forwarder**.
2. On the splunkclouduf Home page, click **Download Universal Forwarder Credentials** to download the `splunkclouduf.spl` file.
3. When prompted, click **Save File** and click **OK**. By default, the `splunkclouduf.spl` file is downloaded to the **Downloads** directory.

17
Open a command prompt window.

4. Navigate to the bin directory of the SplunkUniversalForwarder installation. For example, `cd \Program Files\SplunkUniversalForwarder\bin\`

5. Run the following command (assuming you have added the path to the `splunk` executable to your PATH environment variable): `splunk install app <full path to splunkclouduf.spl> -auth <username>:<password>`

where `<full path to splunkclouduf.spl>` is the path to the directory where the splunkclouduf.spl file is located and `<username>:<password>` are the username and password of an existing admin account on the universal forwarder. Example: `splunk install app \Users\johnsmith\Downloads\splunkclouduf.spl -auth admin:changeme`

6. To restart the universal forwarder, run the following command: `\splunk restart`

**Step 4: Configure data inputs**

To specify the data to be forwarded to Splunk Cloud, perform the following steps.

The steps in this section apply to self-service deployments.

1. In the Splunk Cloud user interface, click **Settings** in the top menu bar.
2. Click **Add Data**.
3. On the Add Data view, click **Forward**.
4. On the **Select Forwarders** page, next to **Select Server Class**, click **New**.
5. Under **Available host(s)**, click one or more forwarder hosts to add to the **Selected host(s)** box. (If your host is not listed, you did not successfully configure your universal forwarder as a deployment client as described in Step 4 above.)
6. In the **New Server Class Name** field, enter a name for the new server class.
7. Click **Next** near the top of the screen.
8. Select the type of data for the universal forwarder to collect. For this example choose **Files & Directories**
9. Enter the name of a file or directory containing data that you want to forward to Splunk Cloud. For example, `c:\Windows\windowsupdate.log`
10. Click **Next**.
11. In the Input Settings view, next to **Source type**, click **Automatic**.
12. Click **Review** and verify your settings are correct.
13. Click **Submit**.
14. To display the data that was forwarded, click **Start Searching**.
For more information about adding data, see Configure the universal forwarder in the Splunk Enterprise Forwarder Manual.

**Forward data to Splunk Cloud from Linux**

To get data into Splunk Cloud, log into your Splunk Cloud deployment and perform the following steps:

1. Download the Splunk Universal Forwarder for Linux.
2. Install the Splunk Universal Forwarder for Linux.
3. Download and install the universal forwarder credentials.
4. Enable forwarder management in Splunk Web. (Self-service Splunk Cloud deployments only.)
5. Configure data inputs, which specify the data to be collected and forwarded.

The following detailed procedure tells you how to install and configure the universal forwarder on a Linux machine.

**Log into your Splunk Cloud deployment**

The way you log in depends on whether your Splunk Cloud deployment is managed or self-service (for details, see Types of Splunk Cloud Deployment.)

**Logging into a self-service Splunk Cloud deployment**

1. In your web browser, go to www.splunk.com.
2. Click My Account.
3. Click Log In.
4. On the Log In page, enter the user name and password provided in your "Welcome" email.
5. Choose My Account > Instances and click Access Instance. The Splunk Cloud user interface displays.

**Logging into a managed Splunk Cloud deployment**

1. In your web browser, go to the URL specified for your deployment. (Your company selected this URL as part of the process of buying Splunk Cloud.)
2. Enter the username and password specified in your Welcome email provided to you by your Splunk administrator.
**Step 1: Download the universal forwarder**

From the Splunk Cloud Home page:

1. In the left sidebar, click **Universal Forwarder**.
2. On the splunkclouduf Home page, click **Download Universal Forwarder**.
3. On the **Download Splunk Universal Forwarder** page, click the **Linux** and choose your Linux platform.
4. When prompted, click **Save File** and click **OK** to download the installer as a compressed archive (.tgz file).

**Step 2: Install the universal forwarder**

Install the universal forwarder on the computer that contains or has access to the data that you want to collect and forward to Splunk Cloud. If you want to install the universal forwarder on a different computer, copy the universal forwarder package file to that machine and continue with the steps below.

To install the universal forwarder on a Linux machine:

1. Navigate to the directory where you want to install the universal forwarder.
2. Issue the following command: `tar xvzf <downloadfile>.tgz`.

**Step 3: Download and install the universal forwarder credentials**

To enable the forwarder to send data to Splunk Cloud, you must download the universal forwarder credentials file, which contains a custom certificate for your Splunk Cloud deployment. The universal forwarder credentials are different from the credentials that you use to log into Splunk Cloud.

When you install the credentials file into the universal forwarder, note that the default username and password for a first-time installation of the universal forwarder is admin:changeme. To change the admin password, run the edit user command. For example: `splunk edit user admin -password mynewpassword -auth admin:changeme`.

To install your universal forwarder credentials from the Splunk Cloud Home page:

1. In the left sidebar, click **Universal Forwarder**.
2. On the splunkclouduf Home page, click **Download Universal Forwarder Credentials** to download the `splunkclouduf.spl` file.

3. When prompted, click **Save File** and click **OK**. By default, the `splunkclouduf.spl` file is downloaded to the Downloads directory. If downloaded to a different location, make note of the location.

4. Open a command prompt window.

5. Navigate to the `/bin` subdirectory of the directory where you installed the universal forwarder.

6. Run the following command:
   ```bash
   splunk install app <full path to splunkclouduf.spl> -auth <username>:<password>
   ```
   where `<full path to splunkclouduf.spl>` is the path to the directory where the `splunkclouduf.spl` file is located and `<username>:<password>` are the username and password of an existing admin account on the universal forwarder. The default is **admin:changeme**. For example:
   ```bash
   splunk install app /Users/johnsmith/Downloads/splunkclouduf.spl -auth admin:changeme
   ```

7. To restart the universal forwarder, run the following command:
   ```bash
   /splunk restart
   ```

---

### Step 4: Enable forwarder management in Splunk Web

You can configure a self-service Splunk Cloud instance as a deployment server that distributes updates to forwarders using Splunk Web. To specify the deployment server host name for self-service deployments, use the URL of your Splunk Cloud instance, omitting the leading "https:" and preceding the URL with "input-". Example:
   ```bash
   /Applications/SplunkForwarder/bin/splunk set deploy-poll input-prd-p-gxxnh2qlt7cx.cloud.splunk.com:8089
   ```
   (The default management port is 8089.)

If your Splunk Cloud deployment is a managed deployment and you want to use Splunk Web to manage forwarders, you must run a deployment server on premises, because managed Splunk Cloud deployments do not include a deployment server. When configuring deployment clients for an on-premises deployment server, specify the hostname and port on which you are running the deployment server. For details about setting up deployment servers, see About deployment server and forwarder management.

To register the universal forwarder as a deployment client, run the following commands (assuming you have added the path to the Splunk forwarder installation directory to your PATH environment variable):

1. ```bash
   splunk set deploy-poll <deployment server hostname>:<mgmtPort>.
   ```
2. ```bash
   splunk restart
   ```
Step 5: Configure data inputs

To specify the data to be forwarded to Splunk Cloud, perform the following steps.

The steps in this section apply to self-service deployments.

1. In the Splunk Cloud user interface, click **Settings** in the top menu bar.
2. In the Search view, under **Data** on the right of the screen, click the **Add Data** button.
3. On the Add Data view, click **Forward**.
4. Next to **Select Server Class**, click **New**.
5. Under **Available host(s)**, click one or more forwarder hosts to add to the **Selected host(s)** box.
6. In the **New Server Class Name** field, enter a name for the new **server class**.
7. Click **Next** near the top of the screen.
8. Select the type of data for the universal forwarder to collect. For this example choose **Files & Directories**.
9. Enter the name of a file or directory containing data that you want to forward to Splunk Cloud. For example, /var/log.
10. Click **Next**.
11. In the Input Settings view, next to **Source type**, click **Automatic**.
12. Click **Review** and verify your settings are correct.
13. Click **Submit**.
14. To display the data that was forwarded, click **Start Searching**.

For more information about adding data, see Configure the universal forwarder in the Splunk Enterprise *Forwarder Manual*.

Forward data to Splunk Cloud from MacOS

To get data into Splunk Cloud, log into your Splunk Cloud deployment and perform the following steps:

1. Download the Splunk Universal Forwarder installer for MacOS.
2. Install the universal forwarder.
3. Download and install the universal forwarder credentials.
4. Enable forwarder management in Splunk Web. (Self-service Splunk Cloud deployments only.)
5. Configure data inputs, which specify the data to be collected and forwarded.
The following detailed procedure tells you how to install and configure the universal forwarder on a Macintosh OS X machine.

**Log into your Splunk Cloud deployment**

The way you log in depends on whether your Splunk Cloud deployment is managed or self-service (for details, see Types of Splunk Cloud Deployment.)

**Logging into a self-service Splunk Cloud deployment**

1. In your web browser, go to www.splunk.com.
2. Click **My Account**.
3. Click **Log In**.
4. On the **Log In** page, enter the user name and password provided in your "Welcome" email.
5. Choose **My Account > Instances** and click **Access Instance**. The Splunk Cloud user interface displays.

**Logging into a managed Splunk Cloud deployment**

1. In your web browser, go to the URL specified for your deployment. (Your company selected this URL as part of the process of buying Splunk Cloud.)
2. Enter the username and password specified in your Welcome email provided to you by your Splunk administrator.

**Step 1: Download the universal forwarder**

From the Splunk Cloud Home page:

1. In the left sidebar, click **Universal Forwarder**.
2. On the splunkclouduf Home page, click **Download Universal Forwarder**.
3. On the **Download Splunk Universal Forwarder** page, choose your Macintosh platform.
4. When prompted, click **Save File** and click **OK** to download the installer as a dmg file. By default, the file is saved in the Downloads directory.

**Step 2: Install the universal forwarder**

Install the universal forwarder on the computer that contains or has access to the data that you want to collect and forward to Splunk Cloud. If you want to install the universal forwarder on a different computer, copy the universal forwarder
installer file to that machine and continue with the steps below.

To install the universal forwarder on a MacOS machine:

1. To launch the installer, double-click the dmg file.
2. Double-click the **Install Splunk Universal Forwarder** icon. The **Introduction** dialog displays, indicating the version and copyright information.
3. Click **Continue**.
4. Read the **Software License Agreement** and click **Continue**.
5. Click **Agree** to confirm you accept the software license agreement and to continue with the installation. The **Installation Type** dialog displays, showing a pre-installation summary.
6. Click **Install**.
7. Confirm you want to install new software.
8. Enter your **Username** and **Password** for the machine you are installing the universal forwarder on, and click **Install Software**. The installation completes and indicates the installation was successful.
9. Click **Close**.
10. When prompted, click **OK** to continue. The installation starts and might take a few minutes to complete.
11. When prompted, click **Start Splunk**.
12. Click **OK** to acknowledge the universal forwarder is installed and started.

**Step 3: Download and install the universal forwarder credentials**

To enable the forwarder to send data to Splunk Cloud, you must download the universal forwarder credentials file, which contains a custom certificate for your Splunk Cloud deployment. The universal forwarder credentials are different from the credentials that you use to log into Splunk Cloud.

When you install the credentials file into the universal forwarder, note that the default username and password for a first-time installation of the universal forwarder is admin:changeme. To change the admin password, run the edit user command. For example (assuming you have added the path to the splunk executable to your PATH environment variable): splunk edit user admin -password mynewpassword -auth admin:changeme

To install your universal forwarder credentials from the Splunk Cloud Home page:

1. In the left sidebar, click **Universal Forwarder**.
2. On the Universal Forwarder page, click **Download Universal Forwarder Credentials** to download the `splunkclouduf.spl` file.

3. When prompted, click **Save File** and click **OK**. By default, the `splunkclouduf.spl` file is downloaded to the **Downloads** directory. If downloaded to a different location, make note of the location.

4. Open a terminal window. (To locate the Terminal application, launch Finder and navigate to Applications > Utilities > Terminal.)

5. In the Terminal window, run the following command:

   ```bash
   /Applications/SplunkForwarder/bin/splunk install app <full path to splunkclouduf.spl> -auth <username>:<password>
   ```

   where `<full path to splunkclouduf.spl>` is the path to the directory where the `splunkclouduf.spl` file is located and `<username>:<password>` are the username and password of an existing admin account on the universal forwarder. The default is admin:change. For example,

   ```bash
   /Applications/SplunkForwarder/bin/splunk install app /Users/johnsmith/Downloads/splunkclouduf.spl -auth admin:changeme
   ```

6. To restart the universal forwarder, run the following command:

   ```bash
   /Applications/SplunkForwarder/bin/splunk restart
   ```

### Step 4: Enable forwarder management in Splunk Web

You can configure a self-service Splunk Cloud instance as a deployment server that distributes updates to forwarders using Splunk Web. To specify the deployment server host name for self-service deployments, use the URL of your Splunk Cloud instance, omitting the leading "https://" and preceding the URL with "input-". Example:

```bash
/Applications/SplunkForwarder/bin/splunk set deploy-poll input-prd-p-gxxnh2qlt7cx.cloud.splunk.com:8089
```

(The default management port is 8089.)

If your Splunk Cloud deployment is a managed deployment and you want to use Splunk Web to manage forwarders, you must run a deployment server on premises, because managed Splunk Cloud deployments do not include a deployment server. When configuring deployment clients for an on-premises deployment server, specify the hostname and port on which you are running the deployment server. For details about setting up deployment servers, see About deployment server and forwarder management.

To register the universal forwarder as a deployment client, run the following commands:

1. ```bash
   ./Applications/SplunkForwarder/bin/splunk set deploy-poll <deployment server hostname>:<mgmtPort>.
   ```

2. ```bash
   ./Applications/SplunkForwarder/bin/splunk restart
   ```
Step 5: Configure data inputs

To specify the data to be forwarded to Splunk Cloud, perform the following steps.

The steps in this section apply to self-service deployments.

1. In the Splunk Cloud user interface, click **Settings** in the top menu bar.
2. In the Settings view, under **Data** on the right of the screen, click the **Add Data** button.
3. On the Add Data view, click **Forward**.
4. Next to **Select Server Class**, click **New**.
5. Under **Available host(s)**, click one or more forwarder hosts to add to the **Selected host(s)** box.
6. In the **New Server Class Name** field, enter a name for the new **server class**.
7. Click **Next** near the top of the screen.
8. Select the type of data for the universal forwarder to collect. For this example choose **Files & Directories**
9. Enter the name of a file or directory containing data that you want to forward to Splunk Cloud. For example, `/var/log`
10. Click **Next**.
11. In the Input Settings view, next to **Source type**, click **Automatic**.
12. Click **Review** and verify your settings are correct.
13. Click **Submit**.
14. To display the data that was forwarded, click **Start Searching**.

For more information about adding data, see Configure the universal forwarder in the Splunk Enterprise *Forwarder Manual*.

Forward data from files and directories to Splunk Cloud

This topic tells you how to configure the universal forwarder to forward the data from local files and directories. To configure forwarding, use the commands and parameters listed in the tables below. To start the universal forwarder, go to the `$SPLUNK_HOME/bin/` directory and run the `splunk start` command. After changing settings for a forwarder, you must restart the forwarder by issuing the `splunk restart` command. To verify that the desired data is being forwarded to Splunk Cloud, use the Splunk Web Search app.
To configure forwarding of data in files, use the commands in this table. For details about other options for forwarding data, see the Forwarder Manual.

<table>
<thead>
<tr>
<th>Command</th>
<th>Command syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>add monitor</td>
<td>add monitor &lt;source&gt; [&lt;parameter value] ...</td>
<td>Start monitoring the specified input. The forwarder watches for changes to the specified source and forwards data to your Splunk Cloud deployment until you remove the source. For example, to continuously monitor the files in the <code>/var/log/</code> directory: <code>splunk add monitor /var/log/</code></td>
</tr>
<tr>
<td>edit monitor</td>
<td>edit monitor &lt;source&gt; [&lt;parameter value] ...</td>
<td>Edit a data input that Splunk Cloud is monitoring. For example, to move a log file from the default location to <code>C:\windows\system32\LogFiles\W3SVC</code>, run the following command: <code>splunk edit monitor C:\windows\system32\LogFiles\W3SVC</code></td>
</tr>
<tr>
<td>remove monitor</td>
<td>remove monitor &lt;source&gt;</td>
<td>Stop monitoring the specified input For example, to stop monitoring of the Windows log file that contains all automatic update activity, run the following command: <code>splunk remove monitor C:\Windows\windowsupdate.log</code></td>
</tr>
<tr>
<td>list monitor</td>
<td>list monitor</td>
<td>Displays a list of all configured data inputs.</td>
</tr>
<tr>
<td>add oneshot</td>
<td>add oneshot &lt;source&gt; [&lt;parameter value] ...</td>
<td>Use this command to forward the contents of the specified data source once. For example, the following commands perform a one-time forwarding of the contents of the <code>/var/log/applog</code> directory. <code>splunk add oneshot /var/log/applog</code> or: <code>splunk spool /var/log/applog</code></td>
</tr>
<tr>
<td>or spool</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Parameter</td>
<td>Required</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>----------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| <source>  | Yes      | Specify the path to the file or directory that contains the data you want to monitor or upload.  
The syntax for this parameter is the value. It is not preceded with the `-source` parameter flag. For example, enter `<source>`, not `-source <source>`. |
| sourcetype| No       | Specify a single source type for the data `<source>`. The source type determines how events are formatted and is a default field that is included in all events. |
| hostname or host | No | Specify a single host or host name for the data "<source>". This default field is included in all events. |

### Examples

<table>
<thead>
<tr>
<th>Description</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor the files in the <code>/var/log/</code> directory (Unix)</td>
<td><code>splunk add monitor /var/log/</code></td>
</tr>
<tr>
<td>Monitor <code>C:\Windows\windowsupdate.log</code></td>
<td><code>splunk add monitor source C:\Windows\windowsupdate.log</code></td>
</tr>
<tr>
<td>Monitor the default location for Windows IIS logging.</td>
<td><code>splunk add monitor C:\windows\system32\LogFiles\W3SVC</code></td>
</tr>
<tr>
<td>One-time upload of a file</td>
<td><code>splunk add oneshot /var/log/applog</code></td>
</tr>
<tr>
<td>Monitor a set of log files in a directory, specifying metadata to be used by the Splunk indexers.</td>
<td><code>splunk add monitor /tmp/foo/*.log -index se_test -sourcetype insurgency -host vm_host01</code></td>
</tr>
</tbody>
</table>
Administer Splunk Cloud

Overview of Splunk Cloud administration

In Splunk Cloud, you use Splunk Web to perform administrative tasks. Unlike Splunk Enterprise, you do not have access to the command line or file system of your Splunk Cloud deployment, so cannot use CLI commands or edit .conf files.

For the following tasks, file a ticket using the Support Portal and Splunk Support will work with you to arrange a maintenance window:

- Installing or deleting **Splunk apps**.
- Managing custom transforms
- Managing capabilities and settings for roles
- Any task that requires editing a .conf file directly.

Read more about settings in the Splunk Enterprise *Admin Manual*.

REST API access to Splunk Cloud

Many administrative tasks can be done using the Splunk REST API. Splunk Cloud supports the same REST endpoints as Splunk Enterprise. For details about REST endpoints, refer to the *REST API Reference Manual*. To use the REST API, you must have a paid subscription to Splunk Cloud.

You cannot use SAML authentication with the REST API.

To enable the Splunk REST API and SDKs, submit a support case on the Support Portal to request access. You can specify a range of IP addresses to control who can access the REST API.

- **Managed Splunk Cloud deployments**: Use the following URL:
  https://<deployment-name>.cloud.splunk.com:8089

- **Self-service Splunk Cloud deployments**: To get the required credentials, submit a support case on the Support Portal. After installing the credentials, use the following URL:
  https://input-<deployment-name>.cloud.splunk.com:8089
Splunk Cloud data policies

Splunk Cloud administers your data according to the policies described below.

Data retention

When you send data to Splunk Cloud, it is stored in indexes. Splunk Cloud retains data based on index settings that enable you to specify when data is to be deleted or moved to self storage. To configure different data retention settings for different sources of data, store the data in separate indexes according to the desired retention policy.

By default, data is retained for a maximum of 90 days. If you want to retain data for more than 90 days, contact Splunk Sales to purchase additional storage.

Each index uses two settings to determine when to delete or move your data:

- The maximum size of the index (specified in the Max data size (GB) field on the Indexes page)
- The maximum age of events in the index (specified in the Retention (days) field on the Indexes page)

When the index reaches the specified maximum size or events reach the specified maximum age, the oldest data is deleted or moved to self storage.

For example, suppose the maximum size of the index is set to 100 GB, and the maximum age of events in the index is set to 15 days. If you send 100 GB every day, then data will never be more than one day old, because every day the index reaches its maximum size and the oldest data is deleted or moved. However, if you send only 1 GB every day, the index never reaches its maximum size, so deletion is controlled by the maximum age. Data is never more than 15 days old and the size of the index remains around 15 GB.

Index data is stored in directories called buckets. Data is deleted by deleting entire buckets, not individual events. Buckets have their own settings that limit their size and the age of events in them. A bucket is not deleted until every event in the bucket meets the deletion settings for the index. If you use data self storage, the bucket is not deleted until the data is successfully moved to your self storage location.

For example, suppose the maximum size of the index is set to 10 GB and the maximum age of events in the bucket is set to 15 days. If you send 1 GB every
day to that bucket, then on day 10 the bucket reaches its size limit, and only then are the index settings for deletion respected. If the maximum size of the index is set to 1 GB, the bucket still grows to 10 GB, at which point the bucket is closed and the index retention settings are applied. Because the index exceeds its limit of 1 GB, the 10 GB bucket is deleted.

Because of this logic, you cannot guarantee that data is deleted on a precise schedule by default. If you require data to be deleted on a precise schedule, contact Splunk Technical Support to discuss the options.

To modify your data retention policy, work with Splunk Technical Support to request modifications to the maxTotalDataSizeMB and frozenTimePeriodInSecs attributes.

Data ingestion and daily license usage

Your Splunk Cloud license governs how much data you can load into your Splunk Cloud deployment per day (GMT). To see current and past daily data ingestion information in Splunk Web, use the Monitoring Console app. To do this, choose Apps, click Cloud Monitoring Console and navigate to the License Usage page. Splunk recommends you set up alerts in the system to monitor your license usage.

You can exceed your purchased daily index volume a maximum of five times in a calendar month. If you exceed your daily limit more than five times in a calendar month, what happens depends on the type of Splunk Cloud deployment you have, as follows:

- **Managed Splunk Cloud**: Your Splunk sales representative may work with you to help you reduce your usage to stay within the purchased limit or to purchase the necessary increase. If you are unable or unwilling to abide by the applicable usage limit, you will pay any invoice for excess usage in accordance with your Terms of Service.
- **Self-service Splunk Cloud deployments**: Your Splunk Cloud instance is locked. You can reset a locked instance three times in a 90-day period. To reset a locked instance, go to your Splunk customer portal and click the Unlock License button. To unlock your instance, your Splunk user must have administrator and instance owner level privilege.

If you consistently exceed your licensed limit, contact Splunk Sales to do a benchmark assessment to determine your volume needs and purchase an appropriate plan to handle your volume.
Backup policy

Splunk Cloud maintains a seven-day backup of data and configuration files. Backups run continuously.

Monitor Splunk Cloud deployment health

The Cloud Monitoring Console lets Splunk Cloud administrators view information about the status of your Splunk Cloud deployment. Cloud Monitoring Console dashboards provide insight into how the following areas of your Splunk Cloud deployment are performing:

- search
- indexing
- forwarder connections
- indexer clustering and search head clustering, if applicable
- license usage, if applicable.

Locate the Cloud Monitoring Console

If you have a self-service Splunk Cloud deployment, to find the Cloud Monitoring Console:

1. Click Settings.
2. Click the Cloud Monitoring Console icon on the left.

If you have a managed Splunk Cloud deployment, the Cloud Monitoring Console is an app.

1. From anywhere in Splunk Web, click Apps.
2. Click Cloud Monitoring Console.

On the App Management page, the Cloud Monitoring Console is named splunk_instance_monitoring.

Dashboards

The Splunk Cloud Monitoring Console app provides information about your Splunk Cloud performance. The information is organized into several dashboards.
<table>
<thead>
<tr>
<th>Dashboard</th>
<th>Description</th>
<th>For more information</th>
</tr>
</thead>
</table>
| Overview         | Information about the performance of your Splunk Cloud deployment, including license usage (if applicable), indexing performance, and search performance information. | About license violations in the Splunk Enterprise Admin Manual  
What Splunk Cloud does with your data in Getting Data In  
About jobs and job management |
| Search Usage Statistics | Information about how your users are running searches.                   | Write better searches in the Splunk Enterprise Search Manual  
Configure the priority of scheduled reports in the Reporting Manual |
| Scheduler Activity | Information about how search jobs (reports) are scheduled.                 | Configure the priority of scheduled reports in the Reporting Manual |
| Skipped Searches | Information regarding skipped searches and search errors. This dashboard is available on managed Splunk Cloud deployments. | See Prioritize concurrently scheduled reports in Splunk Web and Offset scheduled search start times in the Reporting Manual, and Troubleshoot high memory usage in the Splunk Enterprise Troubleshooting Manual. |
| Indexing Overview | Incoming data consumption. Look for an indexing rate lower than expected (for example, an indexing rate of 0 with a forwarder outgoing rate of 100). Filter by source type to discover source types that are sending a larger volume than expected. This dashboard is available on managed Splunk Cloud deployments. | |
| User Activity    | Statistical information about users, page views, and apps.                | |
Check your total data retention capacity

When you send data to Splunk Cloud, it is stored in indexes, and you can self-manage your Splunk Cloud index settings using the Indexes page in Splunk Web. Splunk Cloud retains data based on index settings that enable you to specify when data is to be deleted. Data retention capacity space in your Splunk Cloud service is based on the volume of uncompressed data that you want to index on a daily basis. Splunk Cloud provides 90 days worth of data retention capacity with every subscription. For example, if your daily volume of uncompressed data is 100 GB, your Splunk Cloud environment will have 9000 GB (9 TB) of data retention capacity. You can also purchase additional data retention capacity.
The Cloud Monitoring Console (CMC) Indexes and Storage dashboard provides insights into your data use so that you can better understand your current usage and predict future licensing needs.

In the Indexes and Storage dashboard, the CMC provides insights into your data retention based on the uncompressed data you have indexed.

**Steps to find your retention usage and set an alert**

1. Go to **CMC > Indexes and Storage**.

   ![CMC Indexes and Storage Dashboard](image)

2. Take note of your total index size, which displays in the upper right. This represents your total uncompressed data that is currently retained.

   ![Total Uncompressed Data Retained](image)

3. Compare this value to your licensed entitlement amount to see if you need to update your license based on current usage. If you do not know your licensed entitlement, reach out to your Splunk sales representative.

4. Finally, create a query against CMC, and configure Splunk Cloud to generate an alert if the value exceeds your licensed usage. The following sample query shows the alert where `license_gb=10000000` should be replaced with your licensed data ingestion value (in GB):

   ```splunk
   | dbinspect index=* cached=t
   | where NOT match(index, "^_")
   | stats max(rawSize) AS raw_size BY bucketId, index
   | stats sum(raw_size) AS raw_size
   | eval raw_size_gb = round(raw_size / 1024 / 1024 / 1024 , 2),
   | license_gb = 10000000, storage_usage_pct = round(raw_size_gb /
   | license_gb * 100, 2)
   | fields storage_usage_pct
   ```
5. Note that the query should be run against All Time.

More information

For more information about creating indexes, see Manage Indexes. For detailed instructions on creating alerts, see Alerts.

Understand your index data retention capacity

Your licensed data retention capacity is based on two variables: the daily licensed ingestion rate (e.g. 1 TB per day) and the amount of time Splunk Cloud is licensed to retain your data (e.g. 30 days). To understand how your data retention compares to your licensed retention, it’s a good idea to view details about your index storage.

When you configure data retention for an index, you also configure two variables: the size of the index, and the number of days to retain the data. For example, you set data retention for 10 TB or 90 days, whichever comes first. If your data is retained for less time than you configured, it’s likely that your ingestion rate is higher than expected. For example, if you configured your index to store data for 90 days or 10 TB, and you see that the data is being retained for 10 days, it’s likely that you have hit the 10 TB threshold much sooner than expected, indicating a high ingestion rate. On the other hand, a longer retention than expected could indicate a misconfiguration of your index settings (i.e., you configured data retention for a time period that exceeds your licensed retention).

Steps to investigate your indexes

<table>
<thead>
<tr>
<th>Steps</th>
<th>Detailed Image</th>
</tr>
</thead>
<tbody>
<tr>
<td>Go to CMC &gt; Indexes and Storage.</td>
<td><img src="image" alt="Detailed Image" /></td>
</tr>
</tbody>
</table>
A good method to determine if your data usage is running higher than expected is to check the date of the first event and the date of the last event and compare it to the retention setting for the individual index. For example, if the first event is 12/13/17, and the last event is 12/23/17 and the retention setting for the index is 90 days, then the data ingestion for the index was met long before the time retention setting was met. So, the data ingestion was greater than anticipated.

Next, check to see which indexes are larger than others. You want to find which index is consuming the most storage and why.

- To do this, check the index size, which shows the uncompressed data retained by the index.
- Click the Index Size (GB) heading to sort the indexes by size.
- Click the name of a larger index to open the Index Details page.

In the Index Details page, you can see if there is a spike or a higher trend line for an index. Both of these data points are clues that will tell you that you may need to adjust index settings or investigate further to determine what is causing the spike.

- If you see a spike or rise in data, sort by source type or host to understand if there is a

<table>
<thead>
<tr>
<th>Steps</th>
<th>Detailed Image</th>
</tr>
</thead>
<tbody>
<tr>
<td>A good method to determine if your data usage is running higher than expected is to check the date of the first event and the date of the last event and compare it to the retention setting for the individual index. For example, if the first event is 12/13/17, and the last event is 12/23/17 and the retention setting for the index is 90 days, then the data ingestion for the index was met long before the time retention setting was met. So, the data ingestion was greater than anticipated.</td>
<td><img src="image1" alt="Earliest Event" /> <img src="image2" alt="Latest Event" /></td>
</tr>
<tr>
<td>Next, check to see which indexes are larger than others. You want to find which index is consuming the most storage and why.</td>
<td><img src="image3" alt="Indexes" /></td>
</tr>
<tr>
<td>- To do this, check the index size, which shows the uncompressed data retained by the index. - Click the Index Size (GB) heading to sort the indexes by size. - Click the name of a larger index to open the Index Details page.</td>
<td>Uncompressed Data Retained by Index</td>
</tr>
<tr>
<td>In the Index Details page, you can see if there is a spike or a higher trend line for an index. Both of these data points are clues that will tell you that you may need to adjust index settings or investigate further to determine what is causing the spike.</td>
<td><img src="image4" alt="Index Details" /></td>
</tr>
<tr>
<td>- If you see a spike or rise in data, sort by source type or host to understand if there is a</td>
<td><img src="image5" alt="Index Details" /></td>
</tr>
</tbody>
</table>
specific cause for the increase.
• You may then need to investigate your host or source to determine if there is an issue.
• If you don’t see spikes or a higher trend line, you do not have an issue with ingestion.

<table>
<thead>
<tr>
<th>Steps</th>
<th>Detailed Image</th>
</tr>
</thead>
</table>
| Check your data quality                    | This topic discusses how to check the quality of your data and how to repair issues you may encounter. However, the concept of data quality depends on what factors you use to judge quality. For the purposes of this document, data quality means that the data is correctly parsed. Your data quality can have a great impact on both your system performance and your ability to achieve accurate results from your queries. If your data quality is degraded enough, it can slow down search performance and cause inaccurate search results. Therefore, it’s important to take the time to check and repair any data quality issues before they become a problem. Generally, data quality issues fall under three main categories:  
  • **Line breaks**. When there are problems with line breaks, the ability to parse your data into the correct separate events that it uses for searching is affected.  
  • **Time stamp parsing**. When there are timestamp parsing issues, the ability to determine the correct time stamp to use for the event is affected.  
  • **Aggregation**. When there are problems with aggregation, the ability to break out fields correctly is affected.  

**Guidelines**

Finding and repairing data quality issues is unique to each environment. However, using these guidelines can help you address your data quality.

• It’s a good idea to check your most important data sources first. Often, you can have the most impact by making a few changes to a critical data source.  
• Data quality issues may generate hundreds or thousands of errors due to one root cause. Therefore, it is recommend that you sort by volume and
work on repairing the source that generates the largest volume of errors first.

- Repairing data quality issues is an iterative process. Repair your most critical datasources first, and then run queries against the source again to see what problems remain.
- For your most critical source, you should ideally resolve all data quality issues. This helps to ensure that your searches are effective and your performance is optimal.
- Run these checks on a regular cadence to keep your system healthy.

**Example**

The following example shows the process of resolving a common data quality issue. The steps to resolve your data quality issues may differ, but you can use this example as a general template for resolving data quality issues.

1. Go to **Cloud Monitoring Console > Indexing > Data Quality** to see the Data Quality dashboard.

2. View the Event Processing Issues by Source Type dashboard. In this example, you can see that the greatest volume of issues are timestamp parsing issues in the `splunk_python` source. Since the `splunk_python` source has the most errors, and most are timestamp errors, we decide to work on timestamp errors. The steps below show you how to resolve timestamp errors.

3. In this example, we are most concerned with timestamp errors in the `syslog` source, so we drill down into that source. Drilling down, we can see that the majority of issues are with the following source:
   `/var/log/suricata/stats.log`.

4. Clicking the source allows us to drill down further, where we can see searches against this source.
5. From here, we can look at a specific event. We can see that the issue is that Splunk was unable to parse the timestamp in the MAX_TIMESTAMP_LOOKAHEAD field.

6. To fix this, we go to **Settings > Source types**.

7. In the filter, enter **syslog** for the source type.

8. Select **Actions > Edit**. The Edit Source Type page opens.

9. Click **Timestamp > Advanced?** to open the Timestamp page for editing. Ensure you are satisfied with timestamp format and the Lookahead settings. In this case, we need to edit the Lookahead settings so that Splunk can parse the timestamp correctly.

10. Returning to the main Edit Source Type page, go to the Advanced menu. From here you can make other changes if needed.
Understand your search performance

Healthy search loads are critical to the performance of your entire Splunk Cloud environment. Understanding search patterns can help you to determine if your search workload is aligned with best practices and optimized for the best performance. Often by looking more deeply into search patterns, you can see if a specific user, search, dashboard, or app is inhibiting your performance. If you encounter an issue, you can then work with users to improve performance. Search performance can be investigated by focusing on some key areas.

- Skipped Searches
- Search runtime

Skipped searches

If you are skipping searches, it can be indicative of problems with your search scheduling or query formation. For example, maybe you have scheduled too many searches to run at the same time, and you can alleviate the problem by staggering the scheduled searches.

You may also find that you have a search that attempts to run before the previously scheduled search has completed. For example, if you schedule Search A to run every five minutes, but the first instance of the search takes 10 minutes to complete, then the next time the search is scheduled to run, it will be skipped because the first search has not yet completed. If this occurs, you may need to adjust the time range (set it to 10 minutes instead of 5), or you may need to optimize your search to align with search best practices to improve performance.

For more information about optimizing searches, see About Optimization.
Lastly, you may have skipped searches because your users have met the threshold for concurrency limits that you set in your Splunk System Limits. This is expected behavior, but it may also indicate that your users need help in optimizing their searches.

**Search runtime**

When searches run for a long time, they may use too much compute and memory, causing an overall slowness of the Splunk instance. This commonly occurs when a few poorly formed searches are taking a large amount of resources. It can also occur if you have a dashboard that is being frequently used by multiple users concurrently. In each of these cases, investigating further can help you to pinpoint the searches that are long-running and determine if you can optimize them. Because each company’s environment is different, it’s not easy to set benchmarks for search performance. Generally, the best way to understand your search performance is to compare your historical search times with your current search times to see if there is a change. If search runtimes have slowed, review changes to your environment and new searches to determine if you need to optimize your searches or environment. For example, you may have added a poorly formed search, or you may have added a dashboard that has attracted a lot of traffic.

**To check for skipped searches**

1. Go to [Cloud Monitoring Console > Search > Skipped Scheduled Searches](#).
2. In the Time Range field, select 24 hours to get a better picture of your searches historically.
3. In the Count of Skipped Searches panel, sort by Reason. Frequently, there are a number of skipped searches for the same reason. Take a note of the primary reason or reasons that searches are skipped.
4. Scroll down to see which report is generating the primary issues, and take note of the report name. If you determine that this is an expected behavior, you don’t need to research any further. But, if the skipped searches are unexpected, continue to the next step.
5. Go to [Settings > Searches Reports and Alerts](#).
6. If you know the App associated with the search or report, you can sort by the App. Otherwise, search by the report or search name.
7. Once you locate the search or report, click on it to open the Edit Search dialog box.
8. At this point, you may need to troubleshoot the formation of the search (look for wild cards, check to see if an index is specified, etc).
9. Or, if you found that scheduling is the problem, go to Edit > Edit Schedule to review the schedule for the search.
10. Verify that the schedule for the report or search is in line with how long the search should take to complete. For example, if the report runs every hour, but it takes 1.5 hours to run the search, the searches will be skipped.

To review searches by user

1. Go to Cloud Monitoring Console > Search > Search Usage Statistics.
2. Change the time frame to widen the scope. For example, set it to week to date.
3. Split the search by users so that you can see if there are a few users that are typically running longer searches.
4. Sort by Cumulative Runtime to see which users have the most cumulative search time.
5. Sort by Median Runtime to see which users are running the median longest searches.
6. Click on the name of the user to drill down into more details about that user’s searches.
7. If the user running the most or longest searches is the system user, you may want to review your applications to make sure that you have optimized them, and that they are providing the expected value. You may discover that some applications are not needed or are not used.

Reviewing this data will give you a better understanding of which users run a large number of searches (or run a few long-running searches). At this point, you may want to review the searches for that user in more detail so that you can better understand if they can be optimized.

For more information about optimizing searches, see About Optimization.

To review long-running searches

1. Go to Cloud Monitoring Console > Search > Search Usage Statistics.
2. Expand the time range to at least 24 hours. Searches are automatically sorted by long-running searches.
3. The Only Ad-Hoc Searches toggle should be set to no. This ensures that you will see scheduled searches, which are more likely to be long-running searches than ad-hoc searches.
4. Scroll down to the Search Details panel where the searches are sorted by search runtime.
5. Click the search name to view more details, and scroll to the bottom of the screen. Two events are displayed. In the second event, you can see the search query.

If you discover a long-running query that runs frequently, you may want to expand the time range to a week or longer to see how commonly this search is run. If it is running frequently, consider optimizing the search.

For more information about optimizing searches, see About Optimization.

**Self-service Splunk Cloud: Enable platform alerts**

The Cloud Monitoring Console for self-service Splunk Cloud provides preconfigured alerts that you can enable. If a platform alert is triggered, the Cloud Monitoring Console displays a notification on the Overview dashboard. In addition, you can set up an alert action (for example, send an email) to be performed when a platform alert is triggered. See Set up alert actions in the *Alerting Manual* for more details.

To enable platform alerts:

1. Go to **Cloud Monitoring Console > Settings > Alerts setup**
2. Click **Enable** next to the alert you wish to enable. Notifications will be displayed in the Overview dashboard.
3. To optionally set up an alert action for the alert, click **Advanced Edit**.

**Manage Splunk Cloud indexes**

Indexes store the data you have sent to your Splunk Cloud deployment. To manage indexes, Splunk Cloud administrators can perform these tasks:

- Create, update, delete, and view properties of indexes.
- Monitor the size of data in the indexes to remain within the limits of a data plan or to identify a need to increase the data plan.
- Modify data retention settings for individual indexes.
- Delete data from indexes.
- Optimize search performance by managing the number of indexes and the data sources that are stored in specific indexes.
- Delete indexes. **Caution:** This function deletes all data from an index and removes the index. The operation is final and cannot be reversed.
• Move expired data from indexes to self storage or a Splunk archive (Dynamic Data Active Archive). Data from the index is not deleted until it is successfully moved to the storage location. Archived data can be restored to Splunk Cloud for searching. Data from a self storage location can no longer be searched from Splunk Cloud. However, it can be restored to a Splunk Enterprise instance for searching if necessary.

**Best practices for creating indexes**

Consider these best practices when creating indexes:

• Create separate indexes for long-term and short-term data. For example, you might need to keep security logs for one year but web access logs for only one month. Using separate indexes, you can set different data retention times for each type of data.
• Apply logical or role-based boundaries for indexes. For example, create separate indexes for different departments.
• Devise a naming convention to easily track, navigate, and organize indexes.
• To configure your data retention settings, see the best practice listed here: Manage Data Retention Settings.

**The Indexes page**

To view the Indexes page, select **Settings > Indexes**. The Indexes page lists the indexes in a Splunk Cloud deployment and allows administrators to create, update, delete, and modify the properties of indexes. To modify settings for an index, click its name.

From this page you can:

• Create an index.
• View index details such as the following.
  ♦ **Index name**: The name specified when the index was created.
  ♦ **Current size (GB)**: The approximate amount of data currently stored in the index.
  ♦ **Max size (GB)**: The maximum amount of raw data (in TB, GB, or MB) retained in the index.
  ♦ **Event count**: The number of events in the index.
  ♦ **Earliest event**: The earliest event found in the index.
  ♦ **Latest event**: The most recent event found in the index.
  ♦ **Searchable Retention (Days)**: The maximum age of events retained in the index.
♦ Status: Enabled or disabled. Data in a disabled index is ignored in searches.
♦ Storage Type: The storage settings for expired data from a given index. Can be self storage, archive, or no additional storage.
♦ Delete an index. Caution: Deletes all data from an index and removes the index. The operation is final and cannot be reversed.

Create a Splunk Cloud index

Splunk Cloud administrators create indexes to organize data, apply role-based access permissions to indexes that contain relevant user data, fine-tune data, specify how long to retain data in indexes, and so on.

1. Select Settings > Indexes.
2. Click New.
3. In the Index Name field, specify a unique name for the index. Names must begin with a lowercase letter or a number and can include uppercase letters, hyphens, and underscores.
4. In the Max data size field, specify the maximum amount of data allowed before data is removed from the index.
5. In the Retention (Days) field, specify the number of days before an event is removed from an index.
6. In the Dynamic Data Storage field, select Splunk Archive to send data to the Splunk Dynamic Data Active Archive, or choose Self Storage to move expired data to your own self-storage area. If you don't want to maintain expired Splunk data, leave No additional storage selected.
7. If you enabled data self storage, select a location for data self storage. Or, click Edit self storage locations to add a new self storage location. For more information about data self storage and instructions for configuring a data self storage location, see Store expired Splunk Cloud data.
8. If you enabled Dynamic Data Active Archive, configure retention settings for the archive. For more information, see Archive expired Splunk Cloud data.
9. Click Save.

The index appears after you refresh the page. Retention settings are applied to individual indexes, and data retention policy settings apply to all of the data that is stored in your Splunk Cloud deployment. Monitor and verify that the data retention settings for all indexes does not meet or exceed the values set in the data retention policy. For more information, see Splunk Cloud data policies.
Manage data retention settings

Each index uses two settings to determine when to delete data:

- The maximum size of the index (GB) (specified in the Max Size of Entire Index field)
- The maximum age of events in the index (specified in the Retention (days) field)

When the index reaches the specified maximum size or events reach the specified maximum age, the oldest data is deleted or is moved to an archive or self-storage location (depending on your configuration).

For example, you ingest data from a particular datasource at a rate of 10 GB per day, and you want to retain and search against the last 90 days worth of data. Given your search and data retention requirements, you should set the values so that the Retention (days) value is reached before the Max Size of Entire Index threshold is reached. Given the above parameters, you might configure the retention settings to the following.

- Max Size of Entire Index set to 1800 GB
- Retention (days) set to 90

These values together account for both your ingestion rate and the time you want to retain the data. You will need to consider these factors for each index that you create.

Finally, it's a good idea to check your data retention in the Cloud Monitoring Console to ensure you estimated your ingestion rate correctly and your storage consumption is within your entitlement. If you did not correctly estimate your ingestion rate, you might have a shorter retention period than expected.

For more information, see Splunk Cloud data policies.

Splunk Cloud administrators can specify the settings that determine when data is removed from a specific index as follows.

For more information about data self storage and instructions for configuring a data self storage location, see Store expired Splunk Cloud data.

For more information about archiving data, see Archive expired Splunk Cloud data.
The new data retention settings appear after you refresh the page.

**Disable a Splunk Cloud index**

Splunk Cloud administrators can disable an index. The data in a disabled index is not queried during searches.

1. Select **Settings > Indexes**.
2. From the **Indexes** page, click **Disable** under the **Status** column.
3. Click **OK** to disable the index.

The index status changes to **Disabled** after you refresh the page. **Note**: You cannot disable default indexes and third-party indexes from the **Indexes** page.

**Enable a Splunk Cloud index**

Splunk Cloud administrators can enable an index. Data in an enabled index can be queried during searches.

1. Select **Settings > Indexes**.
2. Click **OK** to enable the index.

The index status changes to **Enabled** after you refresh the page.

**Delete index data and the index from Splunk Cloud**

Splunk Cloud administrators can delete an index.

**Caution**: This function deletes all data from an index and removes the index. The operation is final and cannot be reversed.

1. Select **Settings > Indexes**.
2. Identify the index and click **Delete** from the **Action** column.
3. Click **OK** to confirm that you want to delete the data and index from Splunk Cloud.

The data and index are deleted from Splunk Cloud and cannot be restored. **Note**: You cannot delete default indexes and third-party indexes from the **Indexes** page.
Store expired Splunk Cloud data

You might need to maintain older data to access it or for compliance purposes. Dynamic Data Self Storage allows you to move your data from your Splunk Cloud indexes to an Amazon S3 bucket in your own AWS environment. You can configure Splunk Cloud to automatically move the data in an index when the data reaches the end of the Splunk Cloud retention period you configure. In addition, you can restore your data to a Splunk Enterprise instance. To ensure there is no data loss, Dynamic Data Self Storage maintains your data in the Splunk Cloud environment until it is safely moved to your configured self storage location.

Requirements for Dynamic Data Self Storage

Dynamic Data Self Storage is available for Managed Splunk Cloud instances only.

To configure a self storage location in an Amazon S3 bucket in your own AWS environment, you need sufficient AWS permissions to create S3 buckets and assign bucket policies to them. If you are not the AWS administrator for your organization, ensure that you are able to work with the AWS administrator during this process to create a new S3 bucket and apply the bucket policy generated by Splunk.

After you move the data to your self storage location, Splunk Cloud does not maintain a copy of this data and does not have access to maintain the data in your self storage environment, so ensure that you understand how to maintain and monitor your data before moving it to your S3 bucket.

The S3 buckets that you use to store your expired Splunk Cloud data must be in the same region as your Splunk Cloud environment. See Create an S3 bucket in your AWS environment for details about creating your S3 bucket.

If you intend to restore your data, you will also need access to a Splunk Enterprise instance.

Performance

Dynamic Data Self Storage is designed to retain your expired data with minimal performance impact. Also, Dynamic Data Self Storage ensures that the export rate does not spike in the case of a large volume of data. For example, if you reduce the retention period from one year to ninety days, the volume increases, but the export rate does not spike. This ensures that changes in data volume
does not impact performance. For more details about Dynamic Data Self Storage performance and limits, see the Splunk Cloud service limits and constraints.

**How Dynamic Data Self Storage works**

Data is moved to your self storage location when the index meets a configured size or time threshold. You may have configured the data to be stored for a certain number of days or until the index reaches a certain size. When that threshold is met, Splunk Cloud attempts to move the data to your configured Amazon S3 bucket. If an error occurs, if there are connection issues, or if the Amazon S3 bucket is unavailable or full, Splunk Cloud attempts to move the data every 15 minutes until it can successfully move it. Splunk Cloud does not delete data from the Splunk Cloud environment until it has successfully moved the data to your self storage location. After the data is stored to your Amazon S3 bucket, you maintain the data using your Amazon S3 tools according to the needs of your organization. If you need to restore the data so that it is searchable, you can restore the data to a Splunk Enterprise instance. The data is restored to a thawed directory, which exists outside of the thresholds for deletion you have configured on your Splunk Enterprise instance. You can then search the data and delete it when you have finished.

When you restore data to a thawed directory on Splunk Enterprise, it does not count against the indexing license volume for the Splunk Enterprise or Splunk Cloud deployment.
Configure self storage locations on Amazon S3

Set up one or more Amazon S3 buckets to store your expired Splunk Cloud data.

Managing self storage locations requires the Splunk indexes_edit capability. All self storage configuration changes are logged in the audit.log file.

Create an Amazon S3 bucket in your AWS environment

In your AWS Management Console, create a new S3 bucket. For information on how to create and manage S3 buckets, search for S3 in the AWS documentation.

Important: the Amazon S3 bucket must be in the same region as your Splunk Cloud environment. When you name the S3 bucket, it must include the prefix provided to you and displayed in the UI before the rest of the bucket name. If you do not use this prefix, Splunk cannot write to your bucket.

By default, your Splunk Cloud instance has a security policy applied which disallows write operations to S3 buckets that do not include your Splunk Cloud ID. This security policy helps ensure that the write operation is allowed only for S3 buckets that you have created for the purpose of storing your expired Splunk Cloud data. If your organization's policies require you to name your S3 buckets without this prefix, open a case with Splunk Support to modify the string limitation.

Access the Self Storage Locations page

1. In Splunk Web, click Settings > Indexes.
2. Click New Index to create a new index, or click Edit in the Actions column for an existing index.
3. In the Dynamic Data Storage field, click the radio button for Self Storage
4. Under the message "No self storage locations have been created yet" click Create a self storage location. Splunk Web opens a new tab to allow you to manage your self storage locations.

Create a self storage location

1. On the Self Storage Locations page, click New Self Storage Location.
2. Give your location a Title and an optional Description.
3. Enter the Amazon S3 bucket name of the S3 bucket that you created.
4. (Optional) Enter the bucket folder name.
5. Click Generate. Splunk Cloud generates a bucket policy.
6. Copy the bucket policy to your clipboard. Do not modify the permissions on the bucket policy.
7. In a separate window, navigate to your AWS Management console and apply this policy to the S3 bucket you created earlier.
8. On the Self Storage Locations page in Splunk Web, click **Test bucket policy**. Splunk Cloud writes a 0KB test file to your S3 bucket to verify that Splunk Cloud has permissions to write to the bucket. A success message displays, and the **Submit** button is enabled.
9. Click **Submit**.
10. In the AWS Management Console, verify that the 0KB test file appears in your bucket.

### Manage self storage settings on an index

Enable Dynamic Data Self Storage on any managed Splunk Cloud index to allow expired data to be stored to an Amazon S3 bucket.

Managing self storage settings requires the Splunk `indexes_edit` capability. All self storage configuration changes are logged in the `audit.log` file.

**Enable self storage for an index**

**Prerequisite**
You must have configured a self storage location. See Configure Self Storage Locations for details.

1. Go to **Settings > Indexes**.
2. Click **New Index** to create a new index, or click **Edit** in the Actions column for an existing index.
3. In the **Dynamic Data Storage** field, click the radio button for **Self Storage**
4. Select a storage location from the drop-down list.
5. Click **Save**.

**Disable self storage for an index**

If you disable self storage for an index, expired data is deleted.

1. Go to **Settings > Indexes**.
2. Click **Edit** in the Actions column for the index you want to manage.
3. In the **Dynamic Data Storage** field, click the radio button for **No Additional Storage**
4. Click **Save**. Self storage is disabled for this index. When data in this index expires, it is deleted.
Disabling self storage for an index does not change the configuration of the external location, nor does it delete the external location or the data stored there. Disabling self storage also does not affect the time or size of the data retention policy for the index.

**Verify Splunk Cloud successfully moved your data**

To verify that your data was successfully moved to your self storage location, you can search the splunkd.log files.

You must have an sc_admin role to search the splunkd.log files.

1. First, you can search your splunkd.log files to view the self storage logs. You search these files in Splunk Web by running the following search.

   ```
   index="_internal" component=SelfStorageArchiver
   ```

2. Next, search to see which buckets were successfully moved to the self storage location:

   ```
   index="_internal" component=SelfStorageArchiver "Successfully transferred"
   ```

3. Verify that all the buckets you expected to move were successfully transferred.

**Monitor changes to self storage settings**

You might want to monitor changes to self storage settings to ensure that the self storage locations and settings meet your company's requirements over time. When you make changes to self storage settings, Splunk Cloud logs the activity to the audit.log. You can search these log entries in Splunk Web by running the following search.

```
index="_audit"
```

Note that Splunk Cloud cannot monitor the settings for the self storage S3 bucket on AWS. For information about monitoring your Amazon S3 buckets, see the Amazon S3 documentation and search for "Monitoring Tools".

The following examples show the log entries available for monitoring your self storage settings.
Log entry for a new self storage location

Splunk Cloud logs the activity when you create a new self storage location. For example:

```
10-01-2017 11:28:26.180 -0700 INFO??AuditLogger -
Audit:[timestamp=10-01-2017 11:28:26.180, user=splunk-system-user,
action=self_storage_enabled, info="Self storage enabled for this
index.", index="dynamic_data_sample" ][n/a]
```

You can search these log entries in Splunk Web by running the following search.

```
index=_audit action=self_storage_create
```

Log entry when you remove a self storage location

Splunk Cloud logs the activity when you remove a self storage location. For example:

```
10-01-2017 11:33:46.180 -0700 INFO??AuditLogger -
Audit:[timestamp=10-01-2017 11:33:46.180, user=splunk-system-user,
action=self_storage_disabled, info="Self storage disabled for this
index.", index="dynamic_data_sample" ][n/a]
```

You can search these log entries in Splunk Web by running the following search.

```
index=_audit action=self_storage_disabled
```

Log entry when you change settings for a self storage location

Splunk Cloud logs the activity when you change the settings for a self storage location. For example:

```
09-25-2017 21:14:21.190 -0700 INFO??AuditLogger -
Audit:[timestamp=09-25-2017 21:14:21.190, user=splunk-system-user,
action=self_storage_edit, info="A setting that affects data retention
was changed." , index="dynamic_data_sample",
setting="frozenTimePeriodInSecs", old_value="440", new_value="5000"
][n/a]
```

The following table shows settings that might change.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>info=&quot;Archiver index setting changed.&quot;</td>
<td>Notification that you successfully changed self storage settings for the specified index.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>index=&quot;dynamic_data_sample&quot;</td>
<td>Name of the index for which self storage settings were modified.</td>
</tr>
<tr>
<td>setting=&quot;frozenTimePeriodInSecs&quot;</td>
<td>The number of seconds before an event is removed from an index. This value is specified in days when you configure index settings.</td>
</tr>
<tr>
<td>old_value=&quot;440&quot;</td>
<td>Value before the setting was updated.</td>
</tr>
<tr>
<td>new_value=&quot;?5000&quot;</td>
<td>Value after the setting has been updated.</td>
</tr>
</tbody>
</table>

You can search these log entries in Splunk Web by running the following search.

index="_audit" action=self_storage_edit

**Restore indexed data from a self storage location**

You might need to restore indexed data from a self storage location. You restore this data by moving the exported data into a thawed directory on a Splunk Enterprise instance, such as $SPLUNK_HOME/var/lib/splunk/defaultdb/thaweddb. When it is restored, you can then search it. You can restore one bucket at a time. Data in the thawed directory is not subject to the server’s index aging scheme, which prevents it from immediately expiring upon being restored. You can put archived data in the thawed directory for as long as you need it. When the data is no longer needed, simply delete it or move it out of the thawed directory.

You cannot restore self storage data to a Splunk Cloud instance. You can restore self storage data only to a Splunk Enterprise instance.

1. Set up a Splunk Enterprise instance. If you have an existing Splunk Enterprise instance, you can use it.
2. Install the AWS CLI tool on your local machine. To find the CLI tool, see AWS Command Line Interface. The AWS CLI tool must be installed in the same location as the Splunk Enterprise instance responsible for rebuilding. The Splunk Enterprise instance can be either local or remote.
3. Configure the AWS CLI tool with the credentials of your AWS self storage location. For instructions on configuring the AWS CLI tool, see the Amazon Command Line Interface Documentation.
4. Use the recursive copy command to download data from the self storage location to the thaweddb directory for your index. You can restore only one
bucket at a time. If you have a large number of buckets to restore, consider using a script to do so. Use syntax similar to the following:

```bash
aws s3 cp s3://<self_storage_bucket>/<self_storage_folder(s)>/<index_name>
/SPLUNK_HOME/var/lib/splunk/<index_name>/thaweddb/ --recursive
```

Make sure you copy all the contents of the archived Splunk bucket because they are needed to restore the data. For example, copy starting at the following level: `db_timestamp_timestamp_bucketID`. Do not copy the data at the level of raw data (.gz files). The buckets display in the `thaweddb` directory of your Splunk Enterprise instance.

5. Restore the indexes by running the following command:

```bash
./splunk rebuild <SPLUNK_HOME>/var/lib/splunk/index_name/thaweddb/<bucket_folder>
```

When the index is successfully restored, a success message displays and additional bucket files are added to the thawed directory, including `tsidx` source types.

After the data is restored, go to the Search & Reporting app, and search on the restored index as you would any other Splunk index.

When you restore data to the thawed directory on Splunk Enterprise, it does not count against the indexing license volume for the Splunk Enterprise or Splunk Cloud deployment.

**Troubleshoot Dynamic Data Self Storage**

When you configure self storage, you might encounter the following issues.

**I don't know the region of my Splunk Cloud environment**

I received the following error when testing my self storage location: *Your S3 bucket must be in the same region as your Splunk Cloud environment <AWS Region>.*

**Diagnosis**

Splunk Cloud detected that you created your S3 bucket in a different region than your Splunk Cloud environment.
Solution

If you are unsure of the region of your Splunk Cloud environment, review the error message. The <AWS Region> portion of the error message displays the correct region to create your S3 bucket. After you determine the region, repeat the steps to create the self storage location.

I received an error when testing the self storage location

When I attempted to create a new self storage location, the following error occurred when I clicked the Test button: Unable to verify the region of your S3 bucket, unable to get bucket_region to verify. An error occurred (403) when calling the Headbucket operation: Forbidden. Contact Splunk Support.

Diagnosis

You might get an error for the following reasons:

• You modified the permissions on the bucket policy.
• You pasted the bucket policy into the incorrect Amazon S3 bucket.
• You did not paste the bucket policy to the Amazon S3 bucket, or you did not save the changes.
• An error occurred during provisioning.

Solution

1. Ensure that you did not modify the S3 bucket permissions. The following actions must be allowed: s3:PutObject, s3:GetObject, s3:ListBucket, s3:ListBucketVersions, s3:GetBucketLocation.
2. Verify that you applied the bucket policy to the correct S3 bucket, and that you saved your changes.
3. If you created the S3 bucket in the correct region, the permissions are correct and you applied and saved the bucket policy to the correct S3 bucket, contact Splunk Support to further troubleshoot the issue.

To review the steps to create the S3 bucket, see ”Create a new self storage location” in this topic.

To review how to apply a bucket policy, see the Amazon AWS S3 documentation and search for ”how do I add an S3 bucket policy?”.
Archive expired Splunk Cloud data

You might need to maintain older data to access it or for compliance purposes. Dynamic Data Active Archive allows you to move your data from your Splunk Cloud indexes to a Splunk-maintained archive. You specify archiving at the index level; i.e., you create an archiving rule for a specified index. This allows you the flexibility to only archive the data that you need to archive. You can configure Splunk Cloud to automatically move the data from an index when the data reaches the end of the Splunk Cloud retention period you configure. In addition, you can restore your data to your Splunk Cloud environment for searching.

Browser Requirements for Dynamic Data Active Archive

Dynamic Data Active Archive supports the same browsers and browser versions supported by Splunk Cloud:

- Firefox ESR (24.2 and current version)
- Internet Explorer 9, 10, and 11 (compatibility mode is not supported)
- Safari (current version)
- Chrome (current version)

How Dynamic Data Active Archive works

Data is moved to the archive when the index meets a configured size or time threshold. You may have configured the data to be stored for a certain number of days or until the index reaches a certain size. When that threshold is met, Splunk Cloud attempts to move the data to the archive location. If an error occurs, if there are connection issues, Splunk Cloud attempts to move the data every 15 minutes until it can successfully move it.

It can take up to 48 hours from the archive initiation for the archiving process to complete.

If an error occurs, the error is logged to the splunkd.log. Splunk Cloud does not delete data from the Splunk Cloud environment until is has successfully moved the data to the archive. If you need to restore the data so that it is searchable, you can restore the data to your Splunk Cloud environment. You can then search the data and delete it when you have finished.
When you restore archived data to Splunk Cloud, it does not count against the indexing license volume for the Splunk Cloud deployment.

**Dynamic Data Active Archive Performance**

When you restore data, it can sometimes impact performance if there is a large amount of data. Splunk Cloud has checks in place to help you determine whether the size of the data is too large to restore, and will provide a warning if the data size may impact performance. Splunk Cloud will block you from restoring an amount of data that could potentially have a very negative impact on performance. If this occurs, select a smaller time range.

**Configure archive settings for an index**

Configure archive settings for a specific index.

Managing archive settings requires the `indexes_edit` capability. All archiving changes are logged in the `audit.log` file.

**Configure archiving for an index**

1. In Splunk Cloud, go to **Settings > Indexes**.
2. Click **New Index** to create a new index or click **Edit** in the Actions column for an existing index.
3. In the Dynamic Data Storage field, select **Splunk Archive**.
4. Set the archive retention period. You can specify this value in years, months, or days. Note that the maximum archive retention period is displayed. This value is based on your licensed archive retention period. Specify a value within this range.
5. Click **Save**.

**Disable archiving for an index**

1. Go to **Settings > Indexes**.
2. Click **Edit** in the Actions column for the index you want to manage.
3. In the Dynamic Data Storage field, select **Self Storage** to move data to self-storage location when it expires or **No Additional Storage** to delete data as it expires.
4. Click **Save**. When data in this index expires, it is deleted.

Disabling archiving for an index does not delete existing archived data. Existing archived data will be maintained until the configured expiration period. Disabling archiving for an index also does not affect the time or size of the data retention
policy for the index.

**Restore archived data to Splunk Cloud**

You might need to restore indexed data from the Splunk archive. When the data is restored, you can then search it like any other data. You restore data based on the time period for the data you want to search. For example, you might want to restore data for a period of a day. When you pick a date from the date-picker, it is treated as 12 a.m. UTC of the selected date. So, if you want to restore one day's worth of archived data, (for example, on 7/10/2018) you would need to specify 07/10/2018 in the ?from field and 07/11/2018 in the ?to field. By default, restored data is searchable for a period of a month and is removed from Splunk after this period. It is not removed from the archive.

After you initiate data restoration, it can take up to 24 hours before data is restored. If it takes longer than 24 hours, contact Splunk Technical Support.

**How restoring data works**

When you restore data to Splunk Cloud from the archive, a copy of the archived data is moved back to the Splunk Cloud environment. To ensure your data is safe, the original archived data is never moved or deleted. This method of temporary data restoration ensures that you can never mistakenly delete your archived data.

When you restore data, Splunk Cloud checks several conditions to ensure that you do not experience performance issues and that you do not duplicate data and cause your queries to return incorrect results:

- **Check for overlapping data.** Splunk Cloud does not restore data if you have already restored data in that same time range. This is to ensure you do not restore duplicate data, which would cause inaccurate search results. For example, if you specify that you want to restore data from 7/1/2018 - 7/3/2018 but you have already restored data from 7/1/2018 - 7/2/2018, Splunk Cloud will prevent your data restore. In this case, it is recommended that you restore that data that falls outside of the range of the data you have already restored. In this example, you would restore data from 7/3/2018-7/4/2018.

- **Check to ensure data is not likely to cause performance issues.** Splunk Cloud checks the size of the data you want to restore and presents you with a warning if the size of the data may cause performance issues. If the size of that data is very likely to cause performance issues, Splunk Cloud will prevent you from restoring the data.
Because there is a time period during which data is being transitioned from Splunk Cloud to the archive, you will not be able to restore that data during the processing period. Generally, the data moved to the archive is available in approximately 48 hours. If your attempt to restore archived data fails, verify that the data was not recently archived.

After the data is temporarily restored to your Splunk Cloud environment it is available for searching for 30 days. To ensure best performance, we recommend that you clear the temporarily restored data when you have finished searching it.

After you have restored data, you may notice that events appear in your index that are older than your configured retention period specifies. This restored data will remain in your index for 30 days or until you clear it.

When you restore archived data to an index in your Splunk Cloud instance, it does not count against the retention periods configured for data in your index. Restored data exists outside of the constraints of retention periods and size limits and does not affect the retention of your existing index data.

**Steps to restore data to Splunk Cloud**

1. In Splunk Cloud, go to **Settings > Indexes**.
2. For the index where you want to restore data, click **Restore**. The menu displays the restore history for the specified index. You can see the history of data restoration and file size for the data restored.
3. Use the date picker to select a time range to retrieve.
4. Click **Check size**. Splunk Cloud checks to see if the size of the file might impact performance. If the file size is too large, Splunk Cloud blocks you from restoring data. If there is a potential performance impact, Splunk Cloud displays a warning. Splunk Cloud also prevents you from restoring data that overlaps with existing restored data.
5. Enter an email address to send job status notifications. Because it can take up to 24 hours to restore data, enter your email address to enable Splunk Cloud to notify you when restoration is complete.
6. Click **Restore** when you have refined the file size or date range to acceptable limits.

It can take up to 24 hours for data to be restored.

7. To check the status of your data restoration, click **Splunk Archive** in the **Storage Type** field to open the Archive page. To view the restore status, click the **Restore** tab. In the **JobStatus** field, you can see the status of your job: Pending (means that the job has been submitted, but has not begun processing), In progress (means that the job has been started, and
is progressing), Success, Cleared (means you successfully deleted the temporary archive from your index), Expired (means that the restored data has passed the 30 day retention period and has been deleted from the index), and Failed. If you receive a Failed status, click the > button for the archive to display more details about why the restoration failed.

**Steps to clear restored data from Splunk Cloud**

Splunk recommends you manually clear restored data when you are finished searching it. To clear restored data:

1. In Splunk Cloud, go to **Settings > Indexes**.
2. Select the index with data you want to clear, and click **Restore** to open the Restore Archive page.
3. For the range of data you want to clear, select **Clear** in the Actions column.

When the data is successfully cleared, the **Jobstatus** column displays a **Cleared** status.

**Monitor Dynamic Data Active Archive**

Splunk generates logs when you archive data and when you restore archived data. You may want to monitor these logs to check for errors during these processes.

**Archiving logs**

To check for error messages that occur when you are archiving data, you can view the coldstoragearchiver entries in the splunkd.log. You can find these entries by running the following search:

```
index=_internal source=*/splunkd.log component=coldstoragearchiver
```

**Data restoration logs**

To check for error messages that occur when you restore archived data, you can view entries in the splunk_archiver_restoration.log, restoration.log, and python.log. You can find these entries by running the following search:

```
index=_internal source=*/splunk_archiver_restoration.log
index=_internal source=*/restoration.log
```
Manage your archives

You can review the status of your archived indexes on the Archived Indexes page.

Steps to review your archived indexes

1. In Splunk Cloud, go to Settings > Indexes.
2. Click Archived Indexes for an archived index to open the Archived Indexes page.
3. Review the indexes you have archived on the Archived tab.
4. To see the restore history for your indexes, click the Restore tab.

On the Restore tab, you can see the indexes that you have restored and their status:

- **Pending.** The request for restoration has been initiated, but has not yet begun.
- **In progress.** The restoration process has started, but it has not been completed.
- **Success.** The data has been successfully restored to your index.
- **Failure.** The restoration failed. Click the > button next to the archive to display more details about the failure.
- **Cleared.** You have successfully cleared the temporarily restored data.
- **Expired.** The restored data has passed the 30 day retention threshold

After you have reviewed the archived indexes, you can determine what actions you want to take for each archived or restored index. You may want to clear archived data or stop archiving an index. Or you may see that a restoration or archive operation failed and chose to troubleshoot the issue.

Troubleshoot Dynamic Data Active Archive

*I received an error when attempting to restore data*

If an error occurs, the error is logged to the splunkd.log. When you review the Archive page, if you experience errors, you may want to review the splunkd.log and specify the coldstoragearchiver component here:

```
index=_internal source=*/python.log
```
I clicked the Check Size button and nothing happened

When restoring data, I clicked the Check Size button multiple times and nothing happened.

Diagnosis

When restoring a large amount of data, it may take some time for Splunk to verify that the size of the data can be restored without causing performance issues. If you click the Check Size buttons multiple times, it may trigger AWS to block the check process.

Solution

Do not click the Check Size button multiple times if you don't immediately receive feedback.

I archived some of my data. When I attempted to restore it a few hours later, the restoration failed.

When I archived data, I attempted to restore it soon after, and the restoration failed.

Diagnosis

Data can take up to 48 hours to archive. If you attempt to restore the data before this time period completes, the restoration will fail.

Solution

Wait until the 48 hour threshold has been met, and then attempt to restore the data.

Manage Splunk Cloud users and roles

Splunk Cloud administrators can create users and assign roles to them. Roles are named collections of capabilities that determine the access and permissions of any user assigned that role. Splunk Cloud comes with predefined user accounts and roles. You can also create custom user accounts and roles.

User accounts that have multiple roles inherit properties from the role with the broadest permissions, as follows.
• **Search filters:** Users that are assigned multiple roles inherit the capabilities from all assigned roles. For example, if you define two roles with different search filters, and a user account is assigned both roles, then the search filters and restrictions of both roles apply to the user. If a user that has no search restrictions is assigned a role that has search restrictions, the user inherits the search restrictions.

• **Allowed indexes:** Users who have multiple roles with multiple indexes assigned get the highest level of index access assigned for any of the roles. For example, if a user is assigned both the "user" role, which limits index access to a single index, and the *power* role, which allows access to all indexes, the user has access to all indexes. If you want the same user account to inherit capabilities from a different "advanced user" role, but nothing more, create a new role specifically for that user.

• **Capabilities:** Users who have multiple roles with multiple capabilities inherit the combined capabilities of all roles. For example if an administrator creates a user account and assigns the "administrator" role with 15 capabilities, and also assigns the "advanced user" role, with a different set of 15 capabilities, the user account has the combined 30 capabilities of both roles.

### Manage Splunk Cloud users

You administer users from the Users page in Splunk Web.

Do not delete or edit the Splunk Cloud system user roles: admin, app-installer, index-manager, internal_ops_admin, and internal_monitoring. Splunk uses these system user roles to perform essential monitoring and maintenance activities. See the section **System User Roles** in this topic for more information.

### Create a Splunk Cloud user account

To create an account for a Splunk Cloud user, perform the following steps:

1. Go to **Settings > Access controls**.
2. In the **Users** row, click **Add New**.
3. Enter a name for the user account in the **Username** field.
4. Enter the first and last name of the user in the **Full name** field.
5. Enter an email address at which you can contact the user in the **Email address** field.
6. Select the time zone for the user. This optionally allows users to view events and other information in their local time zone.
7. (Optional) Set a default app if you want to override the default app that launches after the user logs in. If unset, the user account inherits the
default app that belongs to the role.
8. Assign at least one role to the user or select Create a role for this user to create a new role and assign it to the user. Multiple roles inherit permissions.
9. Enter a temporary password for the user. The password must contain at least eight characters.
10. Reenter the temporary password.
11. Click Save.

The user account appears in the Users page under the Username column. You can contact the user to provide the login credentials needed to access Splunk Cloud. Inform the user to change the temporary password immediately after the first login.

Invite users to your Splunk Cloud instance

If you have a self-service Splunk deployment, invite users to your Splunk Cloud instance as follows:

1. Go to Settings > Access controls.
2. Click Invite Users. The Invite to Splunk dialog is displayed.
3. Enter the name of the user you want to invite, choose the role to be assigned to the user and click Send.

If the desired role isn't listed, cancel the invitation, click the manage product roles link, and add the role. Note that the role must also be defined on the Access controls > Roles page.

Change a Splunk Cloud user account

Splunk Cloud administrators can update user settings.

1. Go to Settings > Access controls.
2. Click Users.
3. Click the username for the user that you want to update.
4. Update the settings and click Save.

Clone a Splunk Cloud user account

Splunk Cloud administrators can clone a user account. The clone operation creates a new user account with the same settings as the cloned user account, except for the username. The username must be unique for each user account.
1. Go to Settings > Access controls.
2. Click Users.
3. Click Clone in the Action column.
4. Enter a unique username for the user in the Username field.
5. Optionally, update additional settings.
6. Click Save.

The new user account appears in the Users page.

Delete a Splunk Cloud user account

Splunk Cloud administrators can delete user accounts.

1. Go to Settings > Access controls.
2. Click Users.
3. Click Delete in the Action column.
4. Click OK.

Manage Splunk Cloud roles

Each user account is assigned one or more roles. Roles give users permissions to perform tasks in Splunk Cloud based on the capabilities assigned to the role. To manage roles, you must be a Splunk Cloud administrator. Do not edit the predefined roles that are provided by Splunk Cloud. Instead, create custom roles that inherit from the built-in roles, and then modify the custom roles as required.

Do not delete or edit the Splunk Cloud system user roles: admin, app-installer, index-manager, internal_ops_admin, and internal_monitoring. Splunk uses these system user roles to perform essential monitoring and maintenance activities. See the section System User Roles in this topic for more information.

Use roles to:

- Restrict the scope of searches.
- Inherit capabilities and available indexes from other roles.
- Specify user capabilities.
- Set the default index or indexes to search when no index is specified.
- Specify which indexes to search.

For more information about capabilities in user roles, see About defining roles with capabilities and List of capabilities in the Securing Splunk Enterprise manual.
Create roles in managed Splunk Cloud deployments

1. Go to Settings > Access controls.
2. Click Roles.
3. Click New.
4. Complete the Add new role form.
5. Click Save.

Create roles in self-service Splunk Cloud deployments

1. Log into Splunk Cloud and go to Settings > Access Controls.
2. Click Roles.
3. Click New and create a custom role with a unique name.
4. Go to the Splunk Customer Portal and click manage product roles.
5. Click Add new.
6. Enter the name of the custom role that you created in Splunk Cloud and click the Save button.

System User Roles

Splunk uses system user roles to perform essential monitoring and maintenance activities.

Do not delete or edit the Splunk Cloud system user roles: admin, app-installer, index-manager, internal_ops_admin, and internal_monitoring.

General abilities of system user roles

The following table provides information about the general abilities of the internal_monitoring and internal_ops_admin system user roles.

<table>
<thead>
<tr>
<th>Ability</th>
<th>internal_ops_admin</th>
<th>internal_monitoring</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search internal data</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Search external data</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manage configurations</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Manage authentication</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manage ingestion</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Restart splunk</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Gather internal metadata</td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>
Configure SAML single sign-on (SSO) to Splunk Cloud

Splunk Cloud lets you use SAML authentication for single sign-on (SSO).

Prerequisites

- A managed deployment of Splunk Cloud. Self-service deployments log in through the Splunk customer portal and cannot independently configure SAML SSO.
- An identity provider configured to provide the role, realName, and mail attributes. Currently, Ping Identity, Okta, Azure AD, and ADFS are the only supported identity providers. If you need help configuring your identity provider, refer to your identity provider’s documentation or support resource.
- An admin role with the change_authentication capability. This permission level lets you enable SAML and edit authentication settings on the Splunk Cloud search head.
- For AD FS, you may need to set the Claim Type as “UPN” when configuring your IdP. The Splunk blog post at https://www.splunk.com/blog/2016/09/14/configuring-microsofts-adfs-splunk-cloud.html provides more information about configuring AD FS for Cloud.

When you configure Splunk Cloud to use your SAML authentication system, you can authorize groups on your SAML server to log in by mapping them to Splunk Cloud roles. To enable SSO, use information provided by your identity provider to configure Splunk Cloud to work with SAML. For details, see Configure single sign-on with SAML in the Securing Splunk Enterprise manual.

Configure hybrid search

You can configure an on-premises Splunk Enterprise search head to connect to both a set of on-premises indexers and a Splunk Cloud indexer cluster. The search head can then run hybrid searches that combine on-premises data with data from Splunk Cloud.
To search across both on-premises and Splunk Cloud data, you must run the search from an on-premises search head. A Splunk Cloud search head can only search data on Splunk Cloud.

**Hybrid search limitations**

The following conditions and limitations apply to hybrid search.

- You must run hybrid searches from an on-premises search head. You cannot run a hybrid search from a Splunk Cloud search head.
- The on-premises search head must run the same version as Splunk Cloud, down to the maintenance level.
- Only ad-hoc searches are supported. Scheduled searches are not supported.
- Hybrid search is not available with any Splunk premium solution, such as Enterprise Security or IT Service Intelligence.

**Enable hybrid search**

This procedure is valid only for an on-premises standalone search head that is not part of either an on-premises indexer cluster or an on-premises search head cluster.

**Prerequisites**

1. Confirm that the on-premises search head is already configured to search across on-premises indexers. To learn how to configure a search head to connect with on-premises indexers, see Deploy a distributed search environment in the Splunk Enterprise Distributed Search manual.
2. Confirm that the on-premises search head is running on the same version of Splunk Enterprise as Splunk Cloud, down to the maintenance level. If necessary, upgrade the search head to the Splunk Cloud version.
3. Go to the Support portal and open a case with Splunk Support to enable hybrid search for your Splunk Cloud instance. Specify that you need:
   - a 1 MB Splunk Enterprise license for the on-premises search head that you want to use for hybrid search
   - the URI for the master node of the Splunk Cloud indexer cluster
   - the security key for the Splunk Cloud indexer cluster

**Steps**

1. Install the 1 MB license on the on-premises search head. See Install a license.
2. Add the following lines to the `server.conf` file on the on-premises search head:

```
[general]
site = site0

[clustering]
multisite = true
master_uri = <master node URI from Support>
mode = searchhead
pass4SymmKey = <security key from Support>
```

3. Restart the search head.

4. Run a search command like the following, which retrieves Splunk log events and lists the indexers that the events come from:

```
index = _* | stats count by splunk_server.
```

If hybrid search is configured correctly, indexers from both your Splunk Enterprise and your Splunk Cloud deployments are listed in the results.

---

**Install apps in your Splunk Cloud deployment**

Splunk apps are composed of pre-built dashboards, reports, alerts, and workflows, optimized for a particular purpose such as monitoring Web servers or network security. Splunk add-ons are a type of app that provide specific capabilities to other apps, such as getting data in, mapping data, or providing saved searches and macros.

Only approved apps and add-ons can be installed in a Splunk Cloud deployment. Approved apps have been examined by Splunk to ensure they comply with the security requirements of Splunk Cloud. To discuss apps that might fit your needs and work well in your deployment, email your Splunk sales representative. For details about developing your own apps, see Build Splunk Apps.

You must be a Splunk Cloud administrator to install and manage apps in your Splunk Cloud deployment.

**Before you install apps**

When you install an app, your Splunk Cloud deployment might need to restart, making it briefly unavailable to your users. Notify users before you install apps, and consider scheduling installation to avoid inconveniencing your users.
Some installation and upgrade tasks require help from Splunk Support. Contact Splunk Support for the following tasks:

- Install an app that is not available for self-service installation.
- Install an app that is not available from Splunkbase.
- Install premium apps (Splunk Enterprise Security, Splunk App for VMware, Splunk MINT, Splunk App for PCI Compliance, and so on).

**Install an app**

The procedure for installing apps and add-ons for use with your Splunk Cloud instance depends on the type of your Splunk Cloud deployment and the version of Splunk Cloud that you are running. Access the version of this documentation that matches the version of your Splunk Cloud deployment, then follow the directions that match your deployment type. If you aren’t sure whether your Splunk Cloud deployment is self-service or managed, see Types of Splunk Cloud deployment.

**Install and manage an app in a self-service Splunk Cloud deployment**

Install an app in a self-service Splunk Cloud deployment as follows:

1. From the Splunk Web home page, click the Apps gear icon.
2. Click **Browse more apps**.
3. Select **Install** to install an app.
   - If the app that you want is not listed, or if the app indicates self-service installation is not supported, contact Splunk Support.
4. Follow the prompts to complete the installation.
5. Consult the app documentation to determine if the app must also be installed on your forwarders. If yes, click **Download** to download the app package and deploy it manually to your forwarders.

Splunk Cloud admins can perform most app management tasks on the Apps page in a self-service Splunk Cloud deployment.

- To upgrade an app, go to **Apps > Manage apps** to access the Apps page, then click the update link in the version column.
- To uninstall an app, file a support case.
- To configure an app, follow its documentation for instructions. Configure apps only on the node in your deployment where configuration is required.
Install and manage an app in a managed Splunk Cloud deployment

Install an app in a managed Splunk Cloud deployment as follows:

1. From the Splunk Web home page, click the Apps gear icon.
2. Click Install Apps.
3. Select Install to install an app.
   If the app that you want is not listed, or if the app indicates self-service installation is not supported, contact Splunk Support.
4. Follow the prompts to complete the installation.

When you install an app with declared dependencies, Splunk Cloud automatically resolves its dependencies through Splunkbase. To learn more about declaring dependencies, see Splunk Packaging Toolkit.
5. Consult the app documentation to determine if the app must also be installed on your forwarders. If yes, click Download to download the app package and deploy it manually to your forwarders.

Splunk Cloud admins can perform some app management tasks on the App Management page in a managed Splunk Cloud deployment.

- To upgrade an app, click Update from the App Browser page or Update Available from the App Management page to install the new version. After you update an app, you cannot revert to an earlier version. If a new version of your app is available, but the update action is not available for your app, open a support case.
- To uninstall an app, go to Apps > Manage apps and click Uninstall. If the Uninstall action is not available for your app, open a support case.
- To display the log of app management activities and the names of the users who performed them, go to Apps > Manage apps and click Install Log.
- For additional app management capabilities, open a support case.
- To configure an app, follow its documentation for instructions. Configure apps only on the node in your deployment where configuration is required.

In managed Splunk Cloud deployments, inputs must be configured on forwarders under your control.

Manage private apps in your Splunk Cloud deployment
Private apps are Splunk apps that are private to your Splunk Cloud deployment. These apps are not publicly available on Splunkbase. Like all Splunk apps, private apps must be approved by Splunk to be installed on your Splunk Cloud deployment. Splunk uses the validation tool AppInspect to determine if apps comply with the security requirements of Splunk Cloud. For information about AppInspect, see Splunk AppInspect tool on the Splunk developer portal.

In managed Splunk Cloud deployments, you can use Splunk App Management to manage and install private apps. You must be a Splunk Cloud administrator to manage and install private apps in your Splunk Cloud deployment. In self-service Splunk Cloud deployments, the Splunk App Management feature is not available. File a Support ticket to install private apps.

Create a private app

Prerequisites

- See the Building Splunk Apps documentation on Splunkbase.
- For information about dependencies, see the Splunk Packaging Toolkit.
- For information about Appinspect, see Splunk AppInspect tool on the Splunk developer portal.

Steps

1. Create an app that conforms to Splunk app standards and requirements.
2. Make sure the app package does not have any static dependencies, because only dynamic dependencies are supported.
3. Package the app as a .tgz, .spl, .zip or .gz file. Keep the package size limited to 128MB.
4. Run the app through AppInspect and make sure it passes all app validation checks.

The file is ready to installed on your Splunk Cloud deployment. If you have a managed Splunk Cloud deployment, you can install and manage your private app yourself. If you have a self-service Splunk Cloud deployment, file a Splunk Support ticket to proceed. If you aren't sure whether your Splunk Cloud deployment is self-service or managed, see Types of Splunk Cloud deployment.

Upload and manage private apps in managed Splunk Cloud deployments

In a managed Splunk Cloud deployment, you can upload, install, update, and
view reports for your private apps.

**Upload a private app**

1. In Splunk Web, click the Apps gear.
2. Click the Uploaded Apps tab.
3. Click Upload App.
4. Enter your splunk.com credentials. These credentials are used to authenticate with AppInspect.
5. Select the consent check box and click Login.
6. Select the private app package that you created.
7. Click Upload.

This uploaded package is private to your Splunk Cloud deployment. It is stored in your Splunk Cloud deployment and not on Splunkbase.

When the package is uploaded successfully, it appears in the table on the Uploaded Apps page. The app name and version appear only when the package passes all AppInspect checks and is approved.
The Uploaded Apps table provides the following information:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>App</td>
<td>If the package is approved, the app name is displayed. If the package is not approved, the file name of the uploaded package is displayed.</td>
</tr>
<tr>
<td>Status</td>
<td>Displays the status of the package in the validation process. For details, see the next section, Status.</td>
</tr>
<tr>
<td>Actions</td>
<td>Shows what actions you can take on the package.</td>
</tr>
<tr>
<td>Date Submitted</td>
<td>Shows when the package was uploaded.</td>
</tr>
<tr>
<td>Version</td>
<td>If the package is approved, the app version is displayed. If the package is not approved, N/A is displayed.</td>
</tr>
</tbody>
</table>

**Status**

Based on the result of the app validation process, status can be one of the following:

- **Vetting** Package is in the validation process.
- **Approved** Package has passed all AppInspect checks and is ready to be installed.
- **Installed** Package is installed on your Splunk Cloud deployment.
- **Rejected** Package did not pass AppInspect checks. This means that either some checks failed, or some manual checks were detected that must be reviewed by the Splunk AppInspect team. Click View Report to see which checks failed.
- **Failed message** Package validation did not complete due to some issues, for example, issues with the AppInspect service. Click More Info to find out why the package failed validation.

**Install a private app**

1. Use the Uploaded Apps table to verify that the status of your package is Approved. Your package must be approved before you can install it.
2. Click Install to install your private app.
3. Click the Apps tab to see that your private app is listed in the Apps table. You can also see that the value for App Origin is Uploaded.
**Update a private app**

1. If you are installing an earlier version, uninstall the currently installed app.
2. Upload your private app.
3. Verify that the app status is **Approved** in the **Uploaded Apps** table.
4. Click **Install** to install an earlier version. Click **Update** to replace an installed app with a later version.
5. Go to the **Apps** tab to see that the later version of your private app is listed in the **Apps** table.

**View Report of a private app**

1. Click **View Report** to see the AppInspect report for your package.
2. Use this report to find out why AppInspect rejected the package.
3. Make the required changes to the package and try uploading again.

**Manage a rolling restart in Splunk Cloud**

Some configuration updates can cause the indexers in your Splunk Cloud deployment to begin a process called a rolling restart. To minimize the impact of a rolling restart, deploy these updates during off-peak hours.

**What users experience during a rolling restart**

A rolling restart means that indexers restart in sequence.

Depending on the details of your data inputs, indexing probably continues. Using forwarders or other types of load balancers, rather than network inputs alone, increases the robustness of your indexing during a rolling restart.

Searches still run during a rolling restart, but they might return incomplete results. Users running searches in Splunk Web receive a message warning of incomplete search results.

**What triggers a rolling restart**

Deploying certain configuration changes triggers a rolling restart. Examples of changes that trigger a rolling restart include, but are not limited to, the following tasks:

- Source type management
• Deleting an index  
• Configuring HTTP Event Collector  
• Installing some apps and add-ons

Adding an index, for example, does not trigger a restart by itself. But if you or another admin has made other configuration changes and not deployed them, then when you deploy your change that adds an index, you also deploy the previous changes. In this way, deploying a seemingly safe change can indirectly trigger a rolling restart.

**Guidance for managing a rolling restart**

To minimize impact to users, deploy configuration changes during times that are off peak for both indexing and searching. You can identify off-peak times from the Snapshots in your Splunk Cloud Monitoring Console. See Monitor Splunk Cloud deployment health.

During a rolling restart, monitor indexing and search performance with the Splunk Cloud Monitoring Console.

**More information**

For more information about how a rolling restart works, see Use rolling restart in the Splunk Enterprise documentation. Note that some of the advanced options are not available by default in Splunk Cloud.

**Upgrade your Forwarders**

If you are using either heavy or universal forwarders, maintaining version compatibility between your forwarders and Splunk Cloud environment ensures there is no interruption to your service. In addition, when forwarders are version compatible with your Splunk Cloud environment, you can immediately take advantage of new capabilities. As a best practice, run the most recent forwarder version, even if the forwarder is a higher version number than your Splunk Cloud environment.

The following are the supported forwarder versions for Splunk Cloud:

<table>
<thead>
<tr>
<th>Forwarder Version</th>
<th>Supported Splunk Cloud Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Forwarder Version</td>
<td>Supported Splunk Cloud Versions</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------------------------------------</td>
</tr>
<tr>
<td>7.2.x</td>
<td>7.0.3+, 7.1.x, 7.2.x</td>
</tr>
<tr>
<td>7.1.x</td>
<td>7.0.3+, 7.1.x, 7.2.x</td>
</tr>
<tr>
<td>7.0.3+</td>
<td>7.0.3+, 7.1.x, 7.2.x</td>
</tr>
<tr>
<td>6.6.x or Less (TLS only)</td>
<td>6.6.3, 7.0.2</td>
</tr>
<tr>
<td>6.6.x or Less (non-TLS)</td>
<td>None</td>
</tr>
</tbody>
</table>

To upgrade your universal forwarder, use the following instructions:

- Upgrade a *nix Universal Forwarder. Upgrade the *nix universal forwarder.
- Upgrade a Windows Universal Forwarder. Upgrade the Windows universal forwarder.

To upgrade your heavy forwarder, use the following instructions:

- Upgrade a Heavy Forwarder on *nix. Upgrade a Heavy Forwarder on *nix.
- Upgrade a Heavy Forwarder on Windows. Upgrade a Heavy Forwarder on Windows.

**Upgrade the *nix universal forwarder**

You have several scenarios for upgrading a *nix universal forwarder:

- Upgrade a single forwarder manually.
- Perform a remote upgrade of a group of forwarders. (Use this option for deployments of any size)

As best practice, run the most recent forwarder version, even if the forwarder is a higher version number than your Splunk Cloud environment.

**Prerequisites to upgrading a *nix universal forwarder**

Read this section before performing an upgrade. Also, see How to upgrade Splunk Enterprise for up-to-date information and potential issues you might encounter when you upgrade Splunk Enterprise.

**Back your files up**

Before you perform the upgrade, back up your configuration files. See Back up configuration information in the Splunk Enterprise Admin Manual.
If you need to revert to an older forwarder release, uninstall the upgrade and reinstall the older release.

Make sure no other processes can start the forwarder automatically

Confirm that you do not have scripts in place to auto-start forwarders. If you do, disable such scripts for now. You can re-enable them later, after the upgrade.

How upgrading works

After you perform the installation of the new forwarder, you must restart it for any changes to take effect. You can run the migration preview utility at that time to see what will change before the files are updated. If you choose to view the changes before proceeding, the forwarder writes the proposed changes to $SPLUNK_HOME/var/log/splunk/migration.log.<timestamp>

Upgrade a single forwarder

There are several packages that you can use to upgrade a universal forwarder. Tar files and pre-built package such as an .rpm, .deb, or .dmg file are available depending on the operating system.

If you use a .tar file to upgrade a forwarder, expand it into the same directory with the same ownership as the existing universal forwarder instance. This overwrites and replaces matching files but does not remove unique files.

If you use an RPM file, use the RPM package manager (rpm -U <splunk_package_name>.rpm) from a shell prompt to perform the upgrade.

If you use a .dmg file (on MacOS), double-click it and follow the instructions. After the installation starts, specify the same installation directory as your existing installation.

On hosts that run AIX, do not use the AIX version of tar to unarchive a tar file during an upgrade. Use the GNU version of tar instead. This version comes with the AIX Toolbox for Linux Applications package that comes with a base AIX installation. If your AIX does not come with this package installed, you can download it from IBM. See IBM AIX Toolbox download information.

1. Stop the forwarder.

   $SPLUNK_HOME/bin/splunk stop
2. Install the universal forwarder package directly over the existing deployment. As a best practice, run the most recent forwarder version, even if the forwarder is a higher version number than your Splunk Cloud environment.

3. Start the forwarder again.

   ```bash
   $SPLUNK_HOME/bin/splunk start
   ```

   The forwarder displays the following:

   This appears to be an upgrade of Splunk.
   ---------------------------------------------------------------
   Splunk has detected an older version of Splunk installed on this machine. To finish upgrading to the new version, Splunk's installer will automatically update and alter your current configuration files. Deprecated configuration files will be renamed with a .deprecated extension.
   You can choose to preview the changes that will be made to your configuration files before proceeding with the migration and upgrade:
   If you want to migrate and upgrade without previewing the changes that will be made to your existing configuration files, choose 'y'.
   If you want to see what changes will be made before you proceed with the upgrade, choose 'n'.
   Perform migration and upgrade without previewing configuration changes? [y/n]

4. Choose whether you want to run the migration preview script to see what changes will be made to your existing configuration files, or proceed with the migration and upgrade right away. If you choose to view the expected changes, the script provides a list of those changes.

5. Once you have reviewed these changes and are ready to proceed with migration and upgrade, run `$SPLUNK_HOME/bin/splunk start` again.

You can complete the last three steps in one line.

- To accept the license and view the expected changes (answer 'n') before continuing the upgrade:

   ```bash
   $SPLUNK_HOME/bin/splunk start --accept-license --answer-no
   ```
• To accept the license and begin the upgrade without viewing the changes (answer 'y'):

```bash
$SPLUNK_HOME/bin/splunk start --accept-license --answer-yes
```

**Perform a remote upgrade**

To perform a remote upgrade, first perform an upgrade on a test machine. Then, create a script to automate the upgrade on remote machines. You can use the sample script that is in the Install a nix universal forwarder remotely with a static configuration topic, but you might need to modify the script to meet the needs of an upgrade.

1. Upgrade the universal forwarder on a test machine, as described in Upgrade a single forwarder.

2. Create a script wrapper for the upgrade commands, as described in Create and execute the script.

3. Run the script on representative target machines to verify that it works with all required shells.

4. Execute the script against the desired set of hosts.

**Upgrade the Windows universal forwarder**

When you upgrade a universal forwarder, the installer updates the software without changing its configuration. You must make any necessary configuration changes after you complete the upgrade. A deployment server can assist in the configuration update process.

There are several forwarder upgrade scenarios:

- You can upgrade a single forwarder with the GUI installer
- You can upgrade a single forwarder with the command line installer
- You can perform a remote upgrade of a group of forwarders (good for deployments of any size)

As a best practice, run the most recent forwarder version, even if the forwarder is a higher version number than your Splunk Cloud environment.
Prerequisites to upgrading a universal forwarder

Confirm that you understand or have all of the following prior to upgrading a forwarder.

Confirm that an upgrade is necessary

Before you upgrade, consider whether you really need to. In most cases, you do not have to upgrade a forwarder. Forwarders are always compatible with later versions of indexers, so you do not need to upgrade them just because you have upgraded the indexers that they send data to.

A case where you might need to upgrade a forwarder is if a later version of the forwarder includes a feature that is not available in the installed forwarder version.

You must perform any platform architecture changes manually

You cannot upgrade a 32-bit version of the universal forwarder with a 64-bit universal forwarder installer. To upgrade from 32-bit to 64-bit, follow these instructions:

1. Back up your configurations, including any apps or add-ons (in %SPLUNK_HOME%/etc/apps). Also back up the checkpoint files located in %SPLUNK_HOME%/var/lib/modinputs.
2. Uninstall the existing 32-bit forwarder, as described in Uninstall the universal forwarder.
3. Install the 64-bit forwarder, as described in Install a Windows Universal Forwarder from an installer.
4. Restore apps, configurations and checkpoints by copying them to the appropriate directories:

   %SPLUNK_HOME%/etc/system/local for configuration files.
   %SPLUNK_HOME%/etc/apps for apps and add-ons.
   %SPLUNK_HOME%/var/lib/modinputs for checkpoint files.

Back your files up

Before you perform an upgrade, back up configuration files. See Back up configuration information in the Splunk Enterprise Admin manual.

There is no means of downgrading to a previous version. If you need to revert to an older forwarder release, uninstall the current version and reinstall the older
Upgrade a single forwarder using the GUI installer

You can upgrade a single forwarder with the GUI installer. The installer stops the forwarder as part of the upgrade process.

1. Download the new MSI file from the universal forwarder download page.
2. Double-click the MSI file. The installer displays the "Accept license agreement" panel.
3. Accept the license agreement and click "Install." The installer upgrades the forwarder, retains the existing configuration, and starts automatically when you complete the installation.

The installer puts a log of upgrade changes in the %TEMP% directory (This is usually the C:\TEMP directory but can be different based on your Windows machine configuration.) It also reports any errors in the Application Event Log.

Upgrade a single forwarder using the command line

You can upgrade a single forwarder by running the command line installer. To upgrade a group of forwarders, load the command line installer into a deployment tool such as Group Policy or System Center Configuration Manager, as described in Perform a remote upgrade.

You cannot make configuration changes during an upgrade. The installer ignores any command line flags that you specify except for the AGREETOLICENSE flag.

1. Download the new MSI file from the Splunk universal forwarder download page.
2. Run msiexec.exe to Install the universal forwarder from the command line.
   - For 32-bit platforms, use
     splunkuniversalforwarder-<...>-x86-release.msi
     msiexec.exe /i
     splunkuniversalforwarder-<...>-x86-release.msi
     [AGREETOLICENSE=Yes /quiet]
   - For 64-bit platforms, use
     splunkuniversalforwarder-<...>-x64-release.msi
     msiexec.exe /i
     splunkuniversalforwarder-<...>-x64-release.msi
     [AGREETOLICENSE=Yes /quiet]
The value of <...> varies according to the particular release, for example, splunkuniversalforwarder-6.3.0-aa7d4b1cc80-x64-release.msi.

3. Wait for the upgrade to complete. The forwarder starts automatically when you complete the installation.

The installer puts a log of upgrade changes in the %TEMP% directory. It also reports any errors in the Application Event Log.

**Perform a remote upgrade of one or more forwarders**

You can use a deployment tool such as Group Policy or System Center Configuration Manager to distribute the forwarder software among a group of forwarders in your environment. You might want to test the upgrade locally on one machine before performing a remote upgrade across all your forwarders.

See Upgrade using the command line, for details on the command line syntax to use in the deployment tool.

The Splunk Enterprise deployment server cannot distribute the universal forwarder, only its apps and configurations. Do not attempt to use deployment server to distribute universal forwarders.

1. Download the new MSI file from the Splunk universal forwarder download page.
2. Load the MSI into your deployment tool. In the tool, specify the command line as follows.
   
   msiexec.exe /i splunkuniversalforwarder-<...>.msi AGREETOLICENSE=Yes /quiet
3. Start the deployment with your deployment tool.
4. Use the deployment monitor to verify that the universal forwarders function properly.

**Upgrade a Heavy Forwarder on *nix**

**Before you upgrade**

Before you upgrade, see About upgrading to 7.2: READ THIS FIRST for information on changes in the new version that can impact you if you upgrade from an existing version.

Your Splunk Heavy Forwarder does not provide a means of downgrading to previous versions. If you need to revert to an older Splunk Forwarder, uninstall
the upgraded version and reinstall the version you want.

**Back your files up**

Before you perform the upgrade, **back up all of your files**.

For information on backing up configurations, see Back up configuration information in the _Splunk Enterprise Admin Manual_.

**How upgrading works**

To upgrade a Heavy Forwarder installation, you must install the new version directly on top of the old version (into the same installation directory.) When the Splunk Heavy Forwarder starts after an upgrade, it detects that the files have changed and asks whether or not you want to preview the migration changes before it performs the upgrade.

If you choose to view the changes before proceeding, the upgrade script writes the proposed changes to the `$SPLUNK_HOME/var/log/splunk/migration.log.<timestamp>` file.

Splunk Heavy Forwarder does not change your configuration until after you restart it.

As a best practice, run the most recent forwarder version, even if the forwarder is a higher version number than your Splunk Cloud environment.

**Upgrade a Splunk Heavy Forwarder**

1. Open a shell prompt on the machine that has the instance that you want to upgrade.
2. Change to the `$SPLUNK_HOME/bin` directory.
3. Run the `$SPLUNK_HOME/bin/splunk stop` command to stop the instance.
4. Confirm that no other processes can automatically start the Splunk Heavy Forwarder.
5. To upgrade and migrate, install the Splunk Heavy Forwarder package directly over your existing deployment.
   - If you use a `.tar` file, expand it into the same directory with the same ownership as your existing Splunk Heavy Forwarder instance. This overwrites and replaces matching files but does not remove unique files. `tar xzf splunk-7.x.x-<version-info>.tgz -C /splunk/parent/directory`
If you use a package manager, such as RPM, type `rpm -U splunk_package_name.rpm`

If you use a .dmg file on Mac OS X, double-click it and follow the instructions. Specify the same installation directory as your existing installation.

6. Run the `$SPLUNK_HOME/bin/splunk start` command.

The Splunk Heavy Forwarder displays the following output.

This appears to be an upgrade of Splunk.

---

Splunk has detected an older version of Splunk installed on this machine. To finish upgrading to the new version, Splunk's installer will automatically update and alter your current configuration files. Deprecated configuration files will be renamed with a .deprecated extension. You can choose to preview the changes that will be made to your configuration files before proceeding with the migration and upgrade:

If you want to migrate and upgrade without previewing the changes that will be made to your existing configuration files, choose 'y'.

If you want to see what changes will be made before you proceed with the upgrade, choose 'n'.

Perform migration and upgrade without previewing configuration changes? [y/n]

7. Choose whether or not you want to run the migration preview script to see proposed changes to your existing configuration files, or proceed with the migration and upgrade right away. If you choose to view the expected changes, the script provides a list.

8. After you review these changes and are ready to proceed with migration and upgrade, run `$SPLUNK_HOME/bin/splunk start` again.

**Upgrade and accept the license agreement simultaneously**

After you place the new files in the Splunk Heavy Forwarder installation directory, you can accept the license and perform the upgrade in one command.

- To accept the license and view the expected changes (answer 'n') before continuing the upgrade, use the following command.

  `$SPLUNK_HOME/bin/splunk start --accept-license --answer-no`

- To accept the license and begin the upgrade without viewing the changes (answer 'y').
Upgrade a Heavy Forwarder on Windows

You can upgrade with either the GUI installer or the msiexec utility on the command line as described in "Install on Windows via the command line".

Splunk does not provide a means of downgrading to previous versions.

After you upgrade Splunk Heavy Forwarder, if you need to downgrade, you must uninstall the upgraded version and then reinstall the previous version of Splunk Heavy Forwarder that you were using. Do not attempt to install over an upgraded installation with an installer from a previous version, as this can result in a corrupt instance and data loss.

As best practice, run the most recent forwarder version, even if the forwarder is a higher version number than your Splunk Cloud environment.

Before you upgrade

Before you upgrade, see About upgrading to 7.2: READ THIS FIRST for information on changes in the new version that can impact you if you upgrade from an existing version.

Splunk Heavy Forwarder does not provide a means of downgrading to previous versions. If you need to revert to an older Splunk Heavy Forwarder release, uninstall the upgraded version and reinstall the version you want.

The Windows domain user must match what you specified at installation

If you installed Splunk Heavy Forwarder with a domain user, you must specify the same domain user explicitly during an upgrade. If you do not, Splunk Heavy Forwarder installs the upgrade as the Local System user. If you do not do this, or you specify the wrong user accidentally during the upgrade, then see Correct the user selected during installation to switch to the correct user before you start Splunk Heavy Forwarder.

Changing Splunk Heavy Forwarder ports during an upgrade is not supported

Splunk Heavy Forwarder does not support changing the management or Splunk Web ports when you upgrade. If you need to change these ports, do so either before or after you upgrade.
Back your files up

Before you upgrade, back up all of your files, including Splunk Heavy Forwarder configurations, indexed data, and binaries.

- For information on backing up configurations, see Back up configuration information in the Admin Manual.

Keep copies of custom certificate authority certificates

When you upgrade on Windows, the installer overwrites any custom certificate authority (CA) certificates that you have created in `%SPLUNK_HOME%\etc\auth`. If you have custom CA files, back them up before you upgrade. After the upgrade, you can restore them into `%SPLUNK_HOME%\etc\auth`. After you have restored the certificates, restart Splunk Heavy Forwarder.

Upgrade a Splunk Heavy Forwarder using the GUI installer

1. Download the new MSI file from the Splunk download page.
2. Double-click the MSI file. The installer runs and attempts to detect the existing version of Splunk Heavy Forwarder installed on the machine. When it locates the older version, it displays a pane that asks you to accept the licensing agreement.
3. Accept the license agreement. The installer then installs the updated Splunk Heavy Forwarder. This method of upgrade retains all parameters from the existing installation. By default, the installer restarts Splunk Heavy Forwarder when the upgrade completes and places a log of the changes made to configuration files during the upgrade in `%TEMP%`.

Upgrade using the command line

1. Download the new MSI file from the Splunk download page.
2. Install the software, as described in Install on Windows via the command line.
   - If Splunk runs as a user other than the Local System user, specify the credentials for the user in your command-line instruction with the LOGON_USERNAME and LOGON_PASSWORD flags.
   - You can use the LAUNCHSPLUNK flag to specify whether Splunk Heavy Forwarder should start up automatically or not when the upgrade finishes, but you cannot change any other settings.
   - Do not change the network ports (SPLUNKD_PORT and WEB_PORT) at this time.
3. Depending on your specification, Splunk Heavy Forwarder might start automatically when you complete the installation.