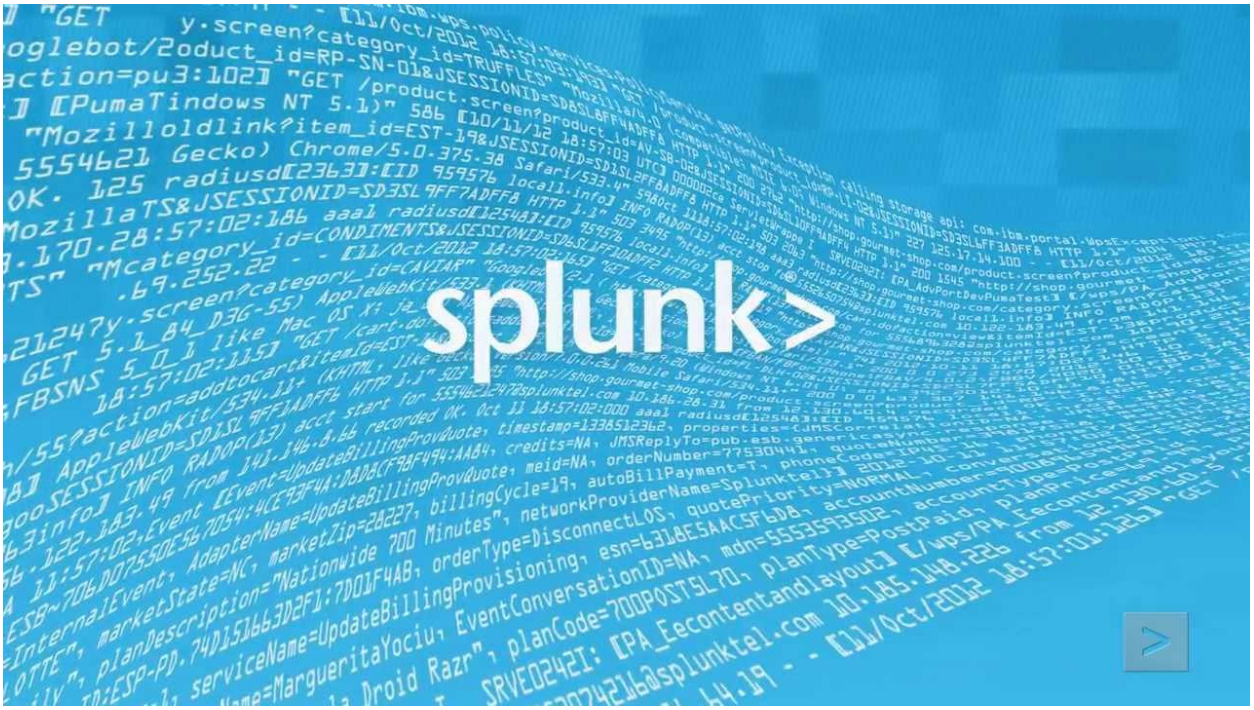
Splunk Employment Guide



Version 1.0
Date: 10-02-2016
POC: @Wired_Pulse

Date	Version	Changelog	Pages	By
10-02-2016	1	Created document	All	@Wired_Pulse

Table of Contents

Introduction

Splunk Enterprise collects and analyzes high volumes of machine-generated data while providing the insight to drive operational performance and results.

Splunkbase is a community hosted by Splunk where users can go to find apps and add-ons for Splunk, which can improve the functionality and usefulness of Splunk, as well as provide a quick and easy interface for specific use-cases and/or vendor products. Splunk apps and add-ons can be developed by anyone, including Splunk themselves.

This document was developed using an instance of Splunk Enterprise on a Windows server machine. As such, all references unless otherwise specified are referring to Windows. For the most part, the same references are applicable to Splunk on any other supported operating system as well.

Splunk Enterprise Installation

Hardware Requirements

Whenever possible, it is recommended that Splunk on ran on the following hardware:

- 2x six-cores
- 2+ GHz CPU
- 12GB RAM
- RAID 0 or 1+0
- 64-bit OS

Software Installation

1. Download the latest version of Splunk Enterprise from www.splunk.com.

2. **Double-click** the Splunk.msi file.

3. **Checkmark** the applicable box to accept the agreement.

4. Click **Install**.

5. Click **Finish**.

6. You will be redirected to the Splunk homepage. (http://localhost:8000).

Loading a Splunk License

1. Click **Settings** in the top right corner.

2. Click **Add License**.

3. Click **Choose File**.

4. Navigate to the license file and select it.

5. Click **Install**.

Configuring a Server Listening Port

1. Click **Settings** in the top right corner.

2. Click **Forwarding and Receiving**.

3. Click **Add New** next to **Configure Receiving**.

4. Input the port that you want Splunk to listen on for data.

5. Click **Save**.

Settings

Within the settings tab, multiple links allow for further configuration and customization of Splunk. While they all will not be addressed here, we will at least address the most commonly used options. Most options listed required very few clicks to configure. Therefore, if the steps are not detailed, that is why.

Knowledge

Searches, Reports, and Alerts

With this option, the following can be accomplished:

- An overview of your searches, reports, and alerts, with options to configure the settings for each of them.
- Once a search is saved, they can be accessed from the Reports tab and quickly executed.
- Alerts can also be created to run a search at a specific time with the results being saved for reviewing later.
- Alerts can also trigger follow on actions such as sending an email if more than five records are returned or execute a specific script based on specified criteria.

To configure a search, do the following:

1. Navigate to **Settings> Search, Reports, and Alerts**.

2. Click **New**.

3. Input the applicable information.

4. Click **Save**.

5. Click on the **Permissions** link on the line containing the new search.

6. Change the saved search option to "All apps". This will make it accessible across all apps.

7. For Roles, give Everyone "**read**" access and Admin "**write**" access.

8. Click **Save**.

To export these searches, see the "Exporting Saved Searches" section linked here.

Tags

In your data, you could have groups of events with related field values. To search more efficiently for these groups of event data, you can assign tags and aliases to your data.

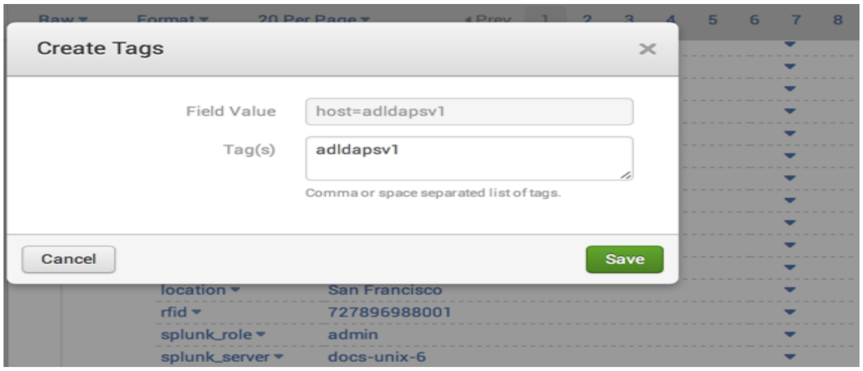
For example. There could be five DNS servers within the organization. Rather than having to search for specific data across all five of those servers, we could add a tag called "DNS" to it. With that done, we could use a search like the below to return data applicable to them.

Example: Tag = DNS

To add a tag to a host field/value combination in your search results:

1. Perform a search for data from the host you would like to tag.

2. In the search results, click on the arrow associated with the event containing the field you want to tag. In the expanded list, click on the arrow under **Actions** associated the field, then select **Edit Tags**.



Create Tags

Field Value: host=adldapsv1

Tag(s): adldapsv1

Comma or space separated list of tags.

location: San Francisco
rfid: 727896988001
splunk_role: admin
splunk_server: docs-unix-6

3. In the Create Tags dialog enter the host field value that you'd like to tag, for example in Field Value enter **Tag host= <current host value>**. Enter your tag or tags, separated by commas or spaces, and click **Save**.

User Interface

Within this menu, multiple interface options can be configured. The most commonly used ones are the following:

- Time Ranges
  - Custom time ranges can be made here and used against searches. Out the box, Splunk has a number of predefined time ranges as well.
- Bulletin Messages
  - Can be set with a custom message that every user logged into Splunk will be notified of. These messages are also listed on the "Messages" tab on the toolbar.

System

- Server Settings
  - General Settings
    - Enables you to change or set various settings such as the following:
      - Change Splunk server name (default is the host name of the system the instance is installed on)
      - Change management port (default is 8089... this is the port the deployment clients use to communicate with the server on)
      - Set single sign-on IP (default has no IP set)
      - Run Splunk Web (default is yes)
      - Enable SSL (default is no)
      - Change web port (default is 8000... this is the port used to access to web interface)
      - Change app server ports
      - Change session timeout (default is set at one hour)

- Customize login page background
  - The Splunk login screen background image can be changed from the default to a custom image or no image at all

- Search preferences
  - The global default time range used for searching is set here.
  - A user does have the ability to temporarily change the time range search criteria for each search that they do.

Server Controls

The Splunk service can be restarted using this window. Splunk could also be restarted by restarting the Splunkd service within services.msc of the local machine.

Licensing

The Splunk license is loaded in this window. Usage is also listed here as well (some of this data can also be found within the "Monitoring Console" (link within Settings). More on loading a license can be found in the "Loading a Splunk License" located here.

Data

Data Inputs

This option allows for the configuration of local inputs for the data we want splunk to index and ingest. Some of the inputs could be log files, files and directories, incoming data on port (syslog), registry monitoring, and custom scripts. On the Splunk homepage, the same options exist when clicking the "Add Data" button.

Note: Although I do not recommend it, we can also do configurations for the deployment client forwarders that are managed by deployment servers here as well. The recommended method can found in the "Updating Deployment Apps" section located here.

Note: If your environment is using forwarders without a deployment server, you will have to manually update each machine if or when the time comes. It is recommended that you use a deployment server to update configurations on a greater scale if you have multiple clients.

Forwarding and Receiving

In the "Receive Data" section, we can configure Splunk to listen on a specific port for incoming data. More on this can be found in the "Configuring a Server Listening Port" section located here.

Splunk also has to ability to send data to and receive data from another Splunk instance. To get that going, do the following:

1. On the sending server, navigate to **Settings> Forwarding and Receiving**.

Note: If you want to save a copy of all forwarded events that you will send, click on **Forwarding Defaults**, then click **Yes**, and then **Save**.

2. Click **Forward Data**.

3. Click **New**.

4. Input the **host:port** you want to forward data to.

5. Click **Save**.

6. On the receiving server, navigate to S**ettings> Forwarding and Receiving**.

7. Configure the system to receive data on the port specified on step 4. To configure a port, see the "Configuring a Server Listening Port" section located here.

Indexes

Indexes are created, deleted, or altered with this option. This is also where you can set the index sizes as well.

Distributed Environment

Forwarder Management

This section is used for managing updates/configurations for deployment clients. For more on this configuration, please see the "Deployment Server Configuration" section located here.

Users and Authentication

Access Controls

Within this option, the following options exist:

- Users
  - Create or delete users
  - Alter user attributes
- Roles
  - Create or delete roles
  - Alter role attributes

Splunk Apps

A Splunk App is a prebuilt collection of dashboards, panels and UI elements powered by saved searches and packaged for a specific technology or use case to make Splunk immediately useful and relevant to different roles. As an alternative to using Splunk for searching and exploring, you can use Splunk Apps to gain the specific insights you need from your machine data. You can also apply user/role based permissions and access controls to Splunk Apps, thus providing a level of control when you are deploying and sharing Apps across your organization. Apps can be opened from the Splunk Enterprise Home Page, from the App menu, or from the Apps section of Settings.

Apps can be downloaded within Splunk in the Apps section or directly from SplunkBase (https://splunkbase.splunk.com/apps/). If downloaded from within Splunk, they will be installed at that time. You will still have to adjust the visibility of the app. See step 7 and 8 of the next section for more details on accomplishing that.

Creating a Custom App

1. Log into the Splunk server.

2. In the system bar, on the upper left, click **Apps > Manage Apps**.

3. Click **Create App** and then click **Add New**.

4. In the Name field, enter a name for the app.

5. In the Folder field, enter a name for the folder.

6. In the Version field, enter a version.

7. In the Visible radio buttons, select **Yes**.

8. In the Author field, type in your name.

9. In the Description field, type in a description for the app.

10. In the Templates list box, choose **barebones**.

11. Click **Save**. Splunk Enterprise saves the app and returns you to the Apps page.

12. In Windows Explorer on the local system, navigate to the default folder (%SPLUNK_HOME%\etc\system\default). Copy the inputs.conf file to the %SPLUNK_HOME%\etc\apps\<newly_created>\local\ directory.

13. Open the **inputs.conf** file with your favorite text editor.

14. Adjust the stanzas for the items you want to collect and for everything else, delete it from the file. The number “1” next to Disabled means it is disabled. Change that to a”0” to enable that item.

15. Save the file.

16. Copy the whole %SPLUNK_HOME%\etc\apps\<newly_created>\ folder to the deployment apps folder.

17. Navigate to **Forwarder Management**.

18. Click the **Server Classes** tab.

19. If you want to add this newly created deployment app to an existing Server Class, do the following:

i. Click on a server class name.
ii. Click on **Edit** near Apps.
iii. Select the app to be added.
iv. Click **Save**.

If you want to add the deployment app to a new server class, do the following:

i. Click New Server Class.
ii. Give it a name and click **Save**.
iii. Click **Add Apps**.
iv. Select the newly created app.
v. Click **Save**.
vi. Click **Add Clients**.
vii. Input the clients to receive this app in the whitelist field.
viii. Click **Preview** and checkmarks should appear by the receiving hosts name in the below pane.
ix. Click **Save**.

20. Open up a PowerShell window and change the directory to **c:\Program Files\Splunk\bin**

21. Reload the deployment server using the below syntax too force the deployment of the new app.

```
PS C:\Program Files\Splunk\bin> .\splunk.exe reload deploy-server –class
"<Server_Class_Name"
```

22. Restart the Splunk forwarder service on all the clients that received app. I have written a PowerShell script that you can run that will do this for you. It is conveniently located on my github (www.github.com/wiredpulse).

23. Within a few minutes, you should data coming into the Splunk server.

Installation (Downloaded Outside of Splunk)

1. Log into Splunk.

2. Click on the **gears** next to Apps in the top left corner of the screen.

3. Click **Install App from File** and hit **Choose File**.

4. Navigate to the .tgz or .zip file and click **Open**.

5. Click **Upload**.

6. Restart the Splunk server when prompted.

7. After logging back in, Click **Edit Properties** in the **Actions** column on the line of your newly installed app.

8. Click **Yes** for visibility and then click **Save**.

Deleting Apps from Splunk

1. Navigate to the %SPLUNK_HOME%\etc\app\ directory.

2. Delete the folder containing the app.

3. Restart the Splunkd service.

Creating Dashboards

Dashboards are views that are made up of panels. The panels can contain modules such as search boxes, fields, charts, tables, and lists. Dashboard panels are usually connected to reports.

After you create a search visualization or save a report, you can add it to a new or existing dashboard. There is also a Dashboard Editor that you can use to create and edit dashboards. The Dashboard Editor is useful when you have a set of saved reports that you want to quickly add to a dashboard.

We will go through creating a dashboard so you will have a basic example as you begin making yours.

Save a Search as a Dashboard Panel

1. Navigate to the search window.

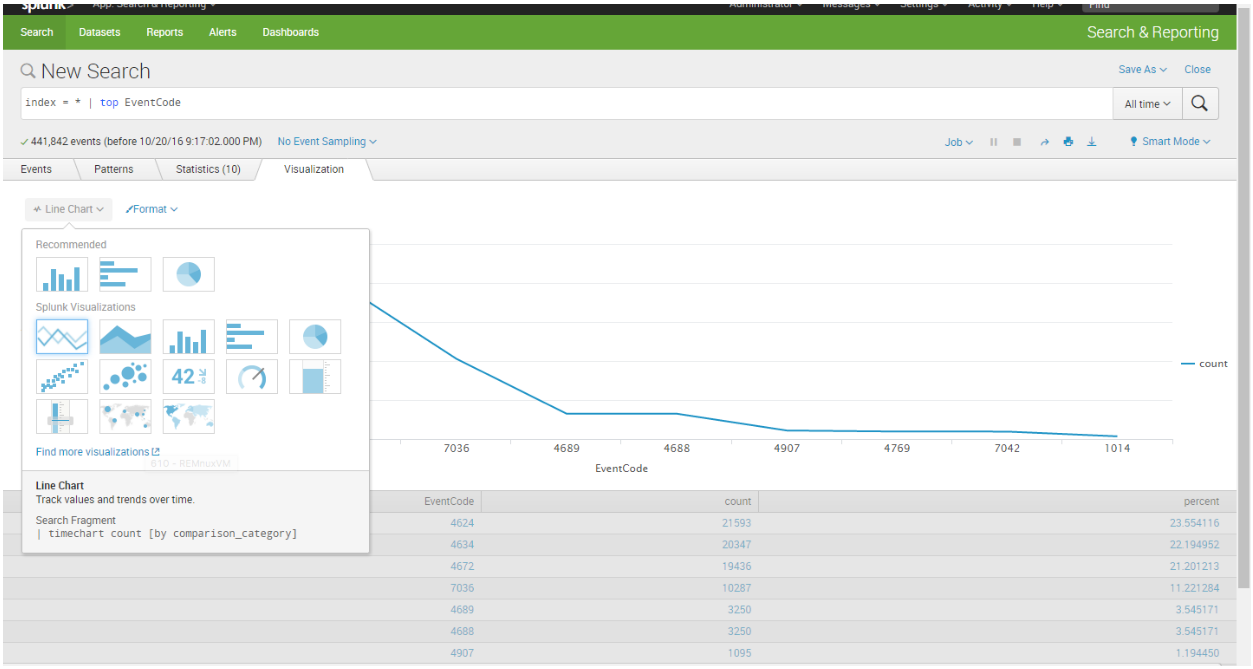
2. Search for “index = * | top “EventCode” (you may not have anything return if you have no data in your Splunk instance).

3. Upon the resulting appearing, we are transitioned to the **Statistics** tab.

4. Click the **Visualization** tab.

5. Our data is present as a Line Chart.

6. Clicking the word “**Line Chart**” in the top left of our graph, we are presented with our visualization options.



```
index = * | top EventCode
```

✓ 441,842 events (before 10/20/16 9:17:02.000 PM) No Event Sampling

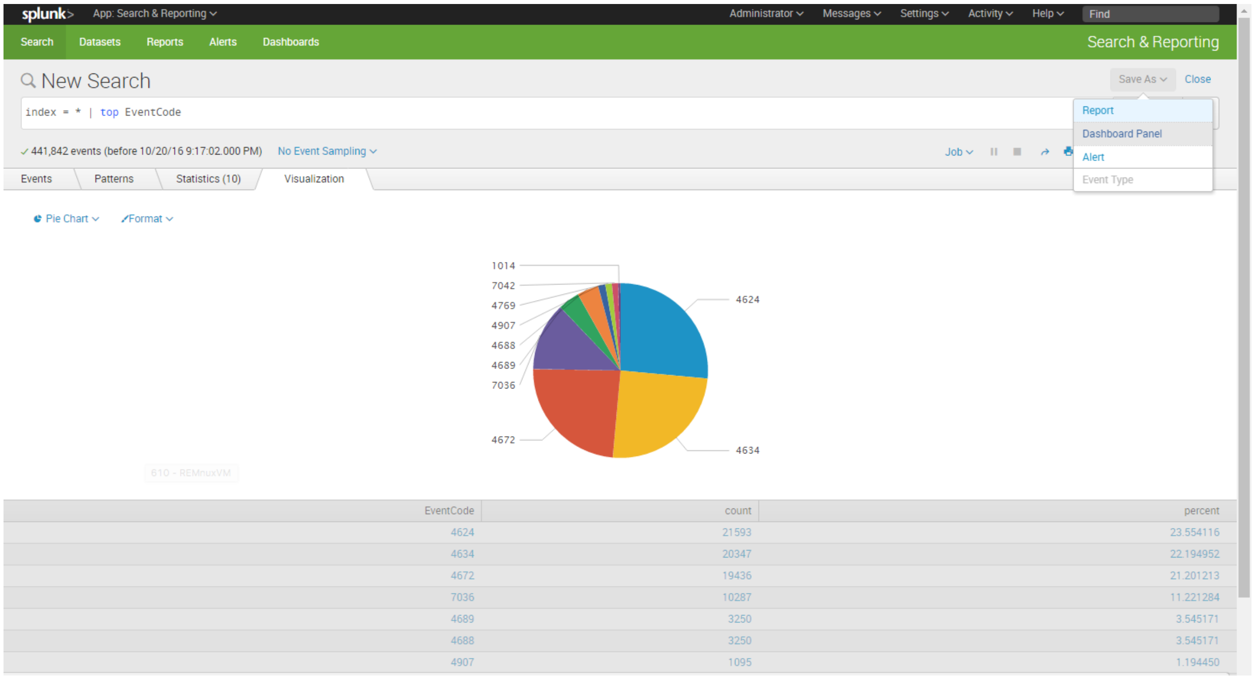
Line Chart
Track values and trends over time.

Search Fragment

```
| timechart count [by comparison_category]
```

EventCode	count	percent
4624	21593	23.554116
4634	20347	22.194952
4672	19436	21.201213
7036	10287	11.221284
4689	3250	3.545171
4688	3250	3.545171
4907	1095	1.194450

7. Change it to Pie Chart.



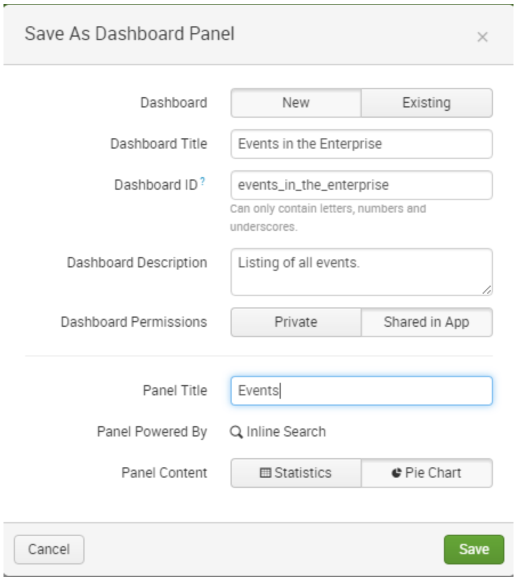
```
index = * | top EventCode
```

✓ 441,842 events (before 10/20/16 9:17:02.000 PM) No Event Sampling

EventCode	count	percent
4624	21593	23.554116
4634	20347	22.194952
4672	19436	21.201213
7036	10287	11.221284
4689	3250	3.545171
4688	3250	3.545171
4907	1095	1.194450

8. In the top right corner of the window, click **Save As > Dashboard Panel**.

9. Click **New**, input a dashboard title and a description, select **Shared in App**, and input a panel title.



Save As Dashboard Panel

Dashboard: New | Existing

Dashboard Title: Events in the Enterprise

Dashboard ID: events_in_the_enterprise
Can only contain letters, numbers and underscores.

Dashboard Description: Listing of all events.

Dashboard Permissions: Private | Shared in App

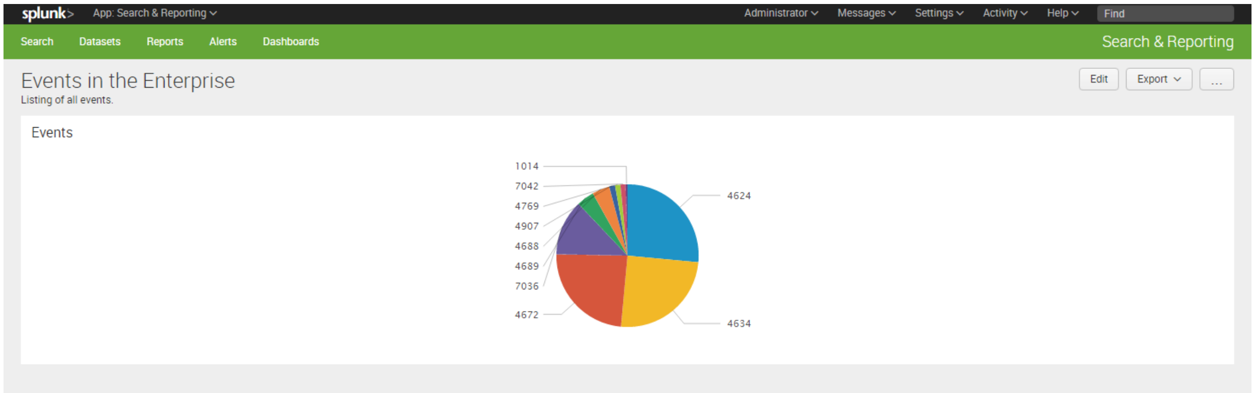
Panel Title: Events

Panel Powered By: Inline Search

Panel Content: Statistics | Pie Chart

10. Click **Save**.

11. Click **View Dashboard**.



Events in the Enterprise
Listing of all events.

Events

You now have a dashboard with one report panel. To add more report panels, you can either run new searches and save them to this dashboard, or you can add saved reports to this dashboard. You will add more panels to this dashboard in the next section.

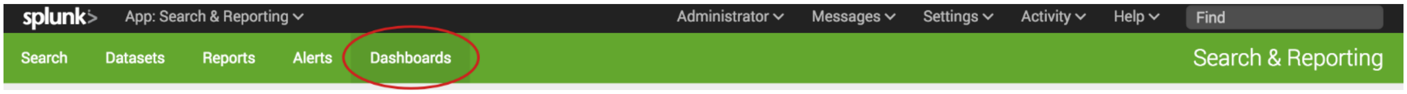
For now, let us spend a little bit more time on this dashboard panel.
View and edit dashboard panels

View and Edit Dashboard Panels

There is a separate view to see a list of the dashboards that you have access to. From this view, you can create dashboards, and make changes to dashboards and dashboard panels.

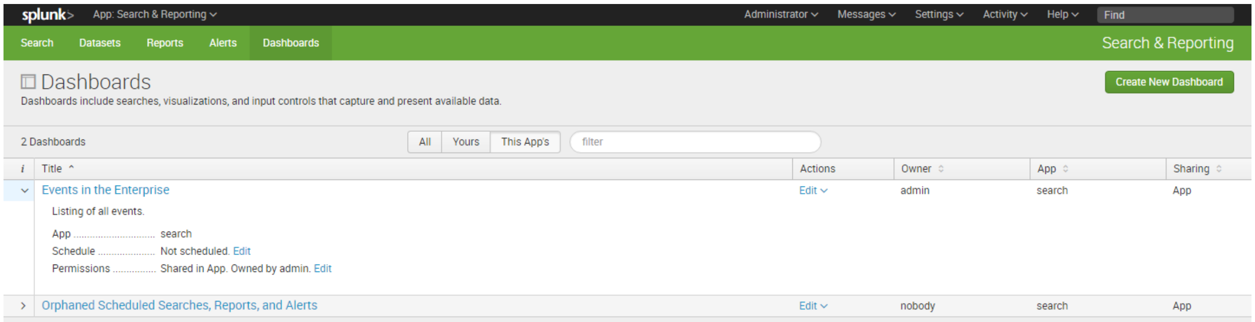
1. Click Dashboards in the App bar to see the Dashboards view.

You might see a pop-up dialog box asking if you want to take a tour about dashboards. If you take the tour, there is an option at the end of the tour to try dashboards yourself. This option displays the Dashboards view.



2. For the Events in the Enterprise dashboard, click the arrow (>) symbol in the *i* column to expand the dashboard information.

You can see information about the app that this dashboard is associated with, whether or not the dashboard is scheduled, and dashboard permissions.



Dashboards

Dashboards include searches, visualizations, and input controls that capture and present available data.

2 Dashboards

i	Title	Actions	Owner	App	Sharing
⌄	Events in the Enterprise	Edit	admin	search	App
>	Orphaned Scheduled Searches, Reports, and Alerts	Edit	nobody	search	App

Listing of all events.

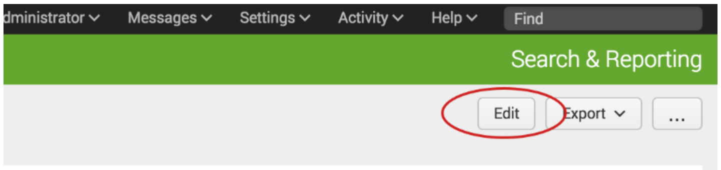
App .... search
Schedule .... Not scheduled. Edit
Permissions .... Shared in App. Owned by admin. Edit

Add Controls to a Dashboard

You can add input controls, such as the Time range picker, to dashboard panels.

1. In the **Dashboards** list, click **Events in the Enterprise** to display that dashboard.

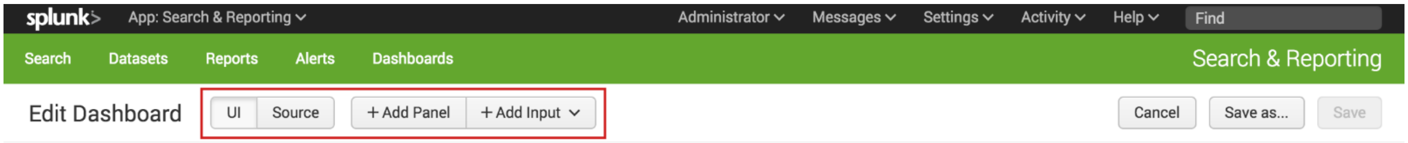
2. Click **Edit**.



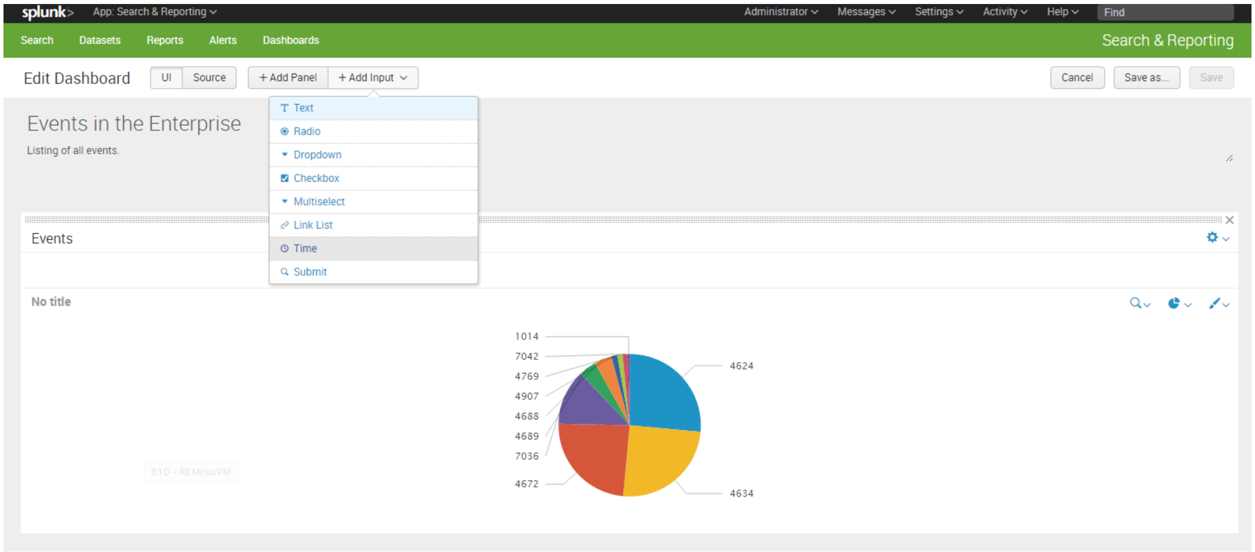
You can either edit the dashboard using the UI or the Source. With the UI option you can add panels and inputs to the dashboard.

- Use the Add Panel option to create a new panel, add a report as a panel, or clone from an existing dashboard.
- Use the Add Input option to choose from a list of controls to add to the dashboard, including text, a checkbox, and a time range picker.

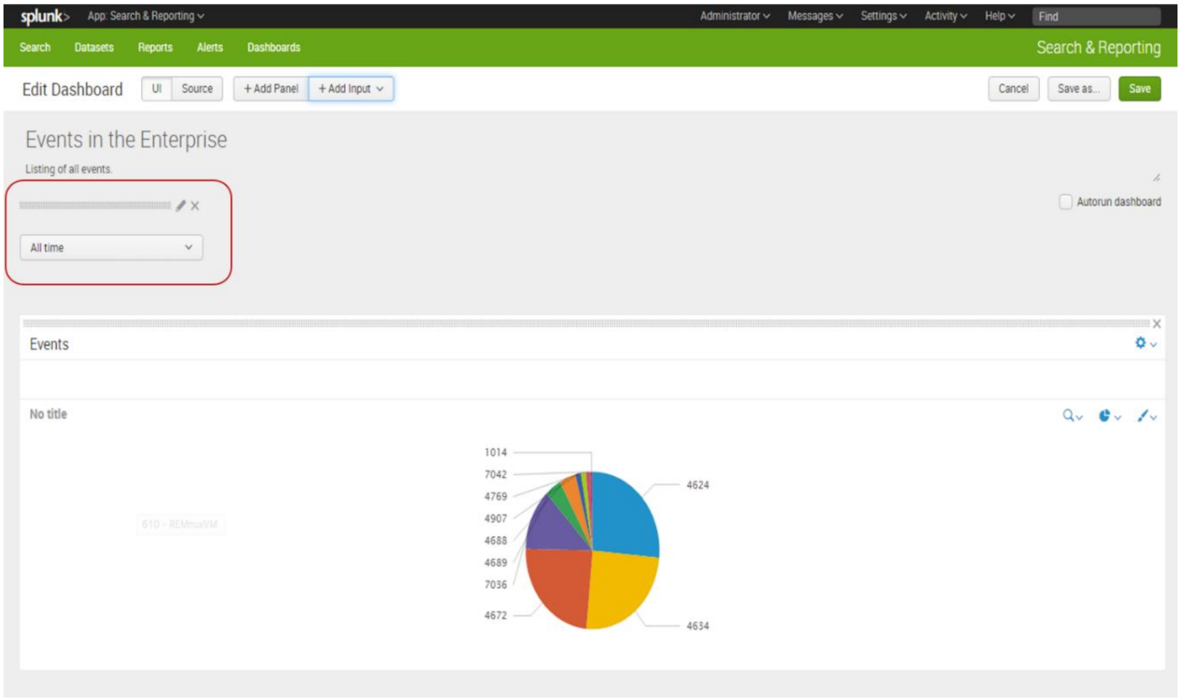
With the Source option, you can edit the XML source for the panel directly. Editing the source directly will not be discussed further in this document.



3. Click **Add Input**, and select **Time**.

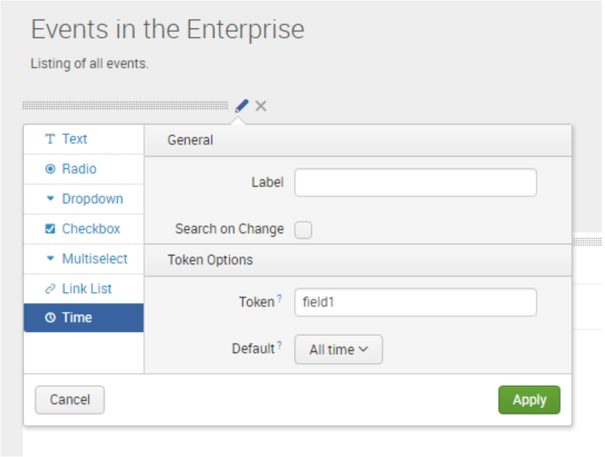


The Time range picker input control appears on the dashboard.



4. Click the **Edit Input** icon for the Time range picker. The icon looks like a pencil.

This opens a set of input controls. The **Time** input type is selected.



Events in the Enterprise

Listing of all events.

General

Label

Search on Change □

Token Options

Token ? field1

Default ? All time

a. For Label, type **Time range**.

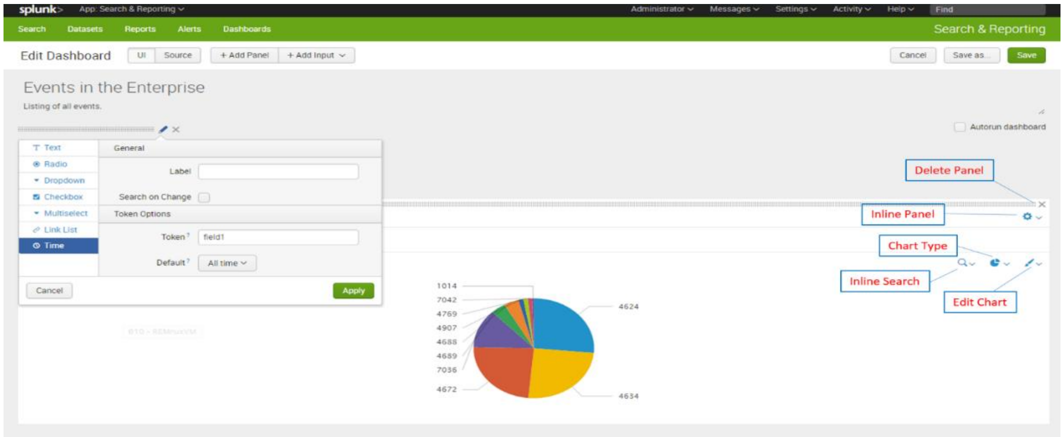
The controls that you add to a dashboard have identifiers called input tokens. This step redefines the name of the input token for the Time range picker. The default names for input tokens are field1, field2, field3, and so on. You can change the input tokens when you add controls to your dashboard.

b. For Default, change the default time range to Previous week.

c. Click Apply.

The input controls that you add to a dashboard are independent from the dashboard panels. If you want the chart on the panel to refresh when you change the time range, you need to connect the dashboard panel to the Time range picker input control.

5. In the dashboard panel, click the **Inline Search** icon.



Edit Dashboard

Events in the Enterprise

Listing of all events.

□ Autorun dashboard

General

Label

Search on Change □

Token Options

Token ? field1

Default ? All time

6. Click **Edit Search**.

7. In the Edit Search dialog box, for **Time Range Scope** select **Shared Time Picker (field 1)**.

8. Click **Apply**.

9. Click **Save** to save the changes to the dashboard.

The panel is now connected to the Time range picker input control in the dashboard. This Time range picker is referred to as the **shared Time range picker**. The inline search that powers the panel now uses the time range that is specified in the shared Time range picker.

NOTE: You can have dashboards that contain a mix of panels. Panels that are connected to the shared Time range picker, and panels that show data for the time range specified in the in the search that the panel is based on. To connect panels to the shared Time range picker, repeat the '''Inline Search > Edit Search''' steps above.

Data Upload

Manual Upload

With Splunk you can manually upload data files, if needed. In order to do so, do the following:

1. Click **Add Data**.

2. Click the **Upload** button.

3. Either hit **Select File** to select a file or drag and drop one on the window.

4. Click **Next**.

5. Set a Source Type as desired for your data and click **Next**.

6. Adjust the input settings as needed and click Review.

7. Click Submit.

Deployment Server Configuration

The preferred method for Splunk usage in an environment with Windows systems is to use a deployment server. In order to configure a deployment server, the following has to be completed:

- Identify a system to serve as the deployment server and install Splunk Enterprise on it
  - Note: The deployment server does not have to be an additional server.
- Create a communication (send to indexer) app on the deployment server, which will be sent to the clients so they know who to communicate with.
- Activate the Splunk instance as a deployment server.
- Configure Server Classes (groups) in order to easily send configurations and apps to a group of systems.
- Install the Universal Forwarder as a deployment client on systems you want to collect data from.
- Configure the deployment server to install the Splunk Add-on for Windows on the deployment clients along with any other apps you desire.

Below are the steps to accomplish it all.

Deployment Server Update Process

The deployment update process works like this:

1. Each deployment client periodically polls the deployment server, identifying itself.

2. The deployment server determines the set of deployment apps for the client, based on which server classes the client belongs to.

3. The deployment server gives the client the list of apps that belong to it, along with those apps' current checksums.

4. The client compares the app info from the deployment server with its own app info, to determine whether there are any new or changed apps that it needs to download.

5. If there are new or updated apps, the deployment client downloads them.

6. Depending on the configuration for a given app, the client might restart itself before the app changes take effect

Key Elements of the Architecture

A **deployment server** is a Splunk Enterprise instance that acts as a centralized configuration manager for any number of other instances, called "deployment clients". Any full Splunk Enterprise instance - even one indexing data locally - can act as a deployment server. A deployment server cannot be a client of itself.

A **deployment client** is a Splunk instance remotely configured by a deployment server. Deployment clients can be universal forwarders, heavy forwarders, indexers, or search heads. Each deployment client belongs to one or more server classes.

A **deployment app** is a set of content (including configuration files) maintained on the deployment server and deployed as a unit to clients of a server class. A deployment app might consist of just a single configuration file, or it can consist of many files. Over time, an app can be updated with new content and then redeployed to its designated clients. The deployment app can be an existing Splunk Enterprise app or one developed solely to group some content for deployment purposes.

Note: The term "app" has a somewhat different meaning in the context of the deployment server from its meaning in the general Splunk Enterprise context.

A **server class** is a group of deployment clients that share one or more defined characteristics. For example, you can group all Windows clients into one server class and all Linux clients into another server class. You use server classes to map a group of deployment clients to one or more deployment apps. By creating a server class, you are telling the deployment server that a specific set of clients should receive configuration updates in the form of a specific set of apps.

"Send to Indexer" App

The "Send to Indexer" app tells the universal forwarders in a Splunk App for Windows Infrastructure deployment to send data to one or more indexers in the deployment. The app prevents you from having to make potentially erroneous configuration changes on many hosts by limiting the change to one place. It also reduces the amount of configuration you have to do on those hosts. The app consists of a single file, **outputs.conf**, that controls where and how the universal forwarders send data.

Creating the outputs.conf File

Before packaging the "Send to Indexer" app, you must first create the **outputs.conf** file. In this procedure, you will create a file that supports sending data to a single indexer.

1. Open Notepad or a similar text editor.

2. In the editor, type in the following text, substituting **indexer_ip_address** with the IP address of the indexer (AKA the Splunk server):

```
[tcpout] defaultGroup = default-autolb-group
[tcpout:default-autolb-group] server = <indexer_ip_address>:9997
[tcpout-server://<indexer_ip_address>:9997]
```

3. Save the file as **outputs.conf** (In Notepad, click **File > Save As…** and type in "outputs.conf" in the file dialog.

Creating the "Send to Indexer" App

The next step of the process is to create the app and upload the **outputs.conf** file you just created as an asset for the app.

1. Log into the Splunk server.

2. In the system bar, on the upper left, click **Apps > Manage Apps**. Splunk Enterprise loads the Apps settings page.

3. Click **Create App**. Splunk Enterprise loads the "Add New" page.

4. In the **Name** field, enter a the name “Send to Indexer”.

5. In the **Folder** field, enter "sendtoindexer".

6. In the **Version** field, enter "1.0.0".

7. In the **Visible** radio buttons, check "No."

8. In the **"Author** field, type in your name.

9. In the **Description** field, type in a description for the app.

10. In the **Templates** list box, choose "barebones".

11. Click **Save**. Splunk Enterprise saves the app and returns you to the Apps page.

Placing the outputs.conf file into the App

Finally, copy the **outputs.conf** file into the app:

1. Open a PowerShell window.

2. Type in the following:

```
PS c:\> Copy-Item -Path <location of outputs.conf> -Destination <Splunk directory>\etc\apps\sendtoindexer\local –Force
```

Activate Deployment Server

1. On the indexer, type the below in PowerShell to move the **sendtoindexer** folder from the Splunk apps directory to the Splunk deployment apps directory.

```
PS c:\> Move-Item -Path C:\Program Files\Splunk\etc\apps\sendtoindexer
-Destination C:\Program Files\Splunk\etc\deployment-apps\sendtoindexer
```

2. From the same command-line prompt, restart Splunk Enterprise:

```
PS c:\> cd C:\Program Files\Splunk\bin
PS c:\> .\splunk restart
```

3. Log back into Splunk Enterprise. The indexer has now gained the deployment server capability.

View Apps in Forwarder Management

Once you have logged back into Splunk, confirm that the deployment server has been activated and is aware of the new "send to indexer" app:

1. In the system bar, click **Settings > Forwarder Management**.

2. Click the **Apps** tab. You should see the "sendtoindexer" app in the list.

Configure a Server Class for the App

The next step is to define a server class for the "send to indexer" app. Server classes are logical data structures that tell deployment servers where and what to send to one or more deployment clients. A server class treats a set of deployment clients as a group - any member of a server class receives apps and configurations defined within that class.

1. From the Apps tab in Forwarder Management, in the **sendtoindexer** listing under **Actions**, click **Edit**. Splunk Enterprise loads the **Edit app: sendtoindexer** page.

2. Click the gray "**+**" sign under **Server Classes**.

3. In the pop-up that appears, click **New Server Class**.

4. In the "New Server Class" dialog box that pops up, enter "Universal Forwarders".

5. Click **Save**. Splunk Enterprise saves the class and loads the information page for the server class you just created.

Note: When you first create a server class, the page says you have not added any apps or clients yet. This is okay.

6. Click **Add apps**. Splunk Enterprise loads the "Edit Apps" page.

7. Locate and click the "sendtoindexer" app in the "Unselected Apps" pane on the left. The app moves to the "Selected Apps" pane on the right.

8. Click **Save**. Splunk Enterprise saves the configuration and returns you to the server class information page.

Install Universal Forwarder as a Deployment Client

In order to begin the data collection and forwarding process, you must install a universal forwarder on every Windows host that you want data from.

Note: Below is depiction of the manual install process. This process can be completed using a PowerShell script I wrote which can be found on my github (www.github.com/wiredpulse).

1. Confirm that your Windows host meets the minimum system requirements for a Splunk universal forwarder installation.

2. Download the appropriate universal forwarder for your version of Windows.

3. Install the universal forwarder onto the Windows host. During the installation process, follow these prompts:

- In the first dialog, check the box to accept the license agreement.
- Click **Customize Options** to customize the installation options.
- Click **Next** to advance through the "Destination Folder" dialog.
- Click **Next** to advance through the "Certificate Information" dialog.
- In the "User selection" dialog, make sure "Local System" is selected and click **Next.**
- In the "Enable Windows inputs" dialog, make sure no inputs have been enabled and click **Next**.
- In the "Specify a Deployment Server" dialog, enter the host name or IP address of the deployment server you just set up in the "**Hostname or IP**" field and enter "**8089**" in the second field. Then click **Next**.
- Click **Next** to advance through the "Receiving Indexer" dialog.
- Click **Install** to accept these configurations and install the universal forwarder.

4. After installation completes, confirm that the universal forwarder service runs.

- You can check the **SplunkForwarder** service in the Services control panel, or

- You can check if the service runs from a PowerShell window (by going to the **%SPLUNK_HOME%\bin** directory and typing in **.\splunk status**.

Adding the Universal Forwarder to the Server Class

This topic discusses adding the universal forwarder you installed in the previous step to the server class you defined on the deployment server. This phase is the final step in configuring the basic infrastructure for the Splunk App for Windows Infrastructure deployment - from here, you can use this procedure to add universal forwarders and server classes as needed.

Universal Forwarder becomes a Deployment Client

When you specified the deployment server during the universal forwarder installation process, the forwarder became what is known as a deployment client. Deployment clients connect to deployment servers and get apps and configurations, then activate and execute those apps and configurations locally.

Earlier, you created the "send to indexer" app, which was an **outputs.conf** file that provided instructions on how to send data to the indexer. You configured this file to send data to the indexer you set up at the beginning of this process. Now, you will complete the loop and deploy the app to any deployment clients that connect to the deployment server.

Confirming that Deployment Server can see the Deployment Client

The first part of this final step is to confirm that the universal forwarder you just installed phones home to the deployment server, which by default is every 30 seconds.

1. Log into the Splunk indexer you set up previously.

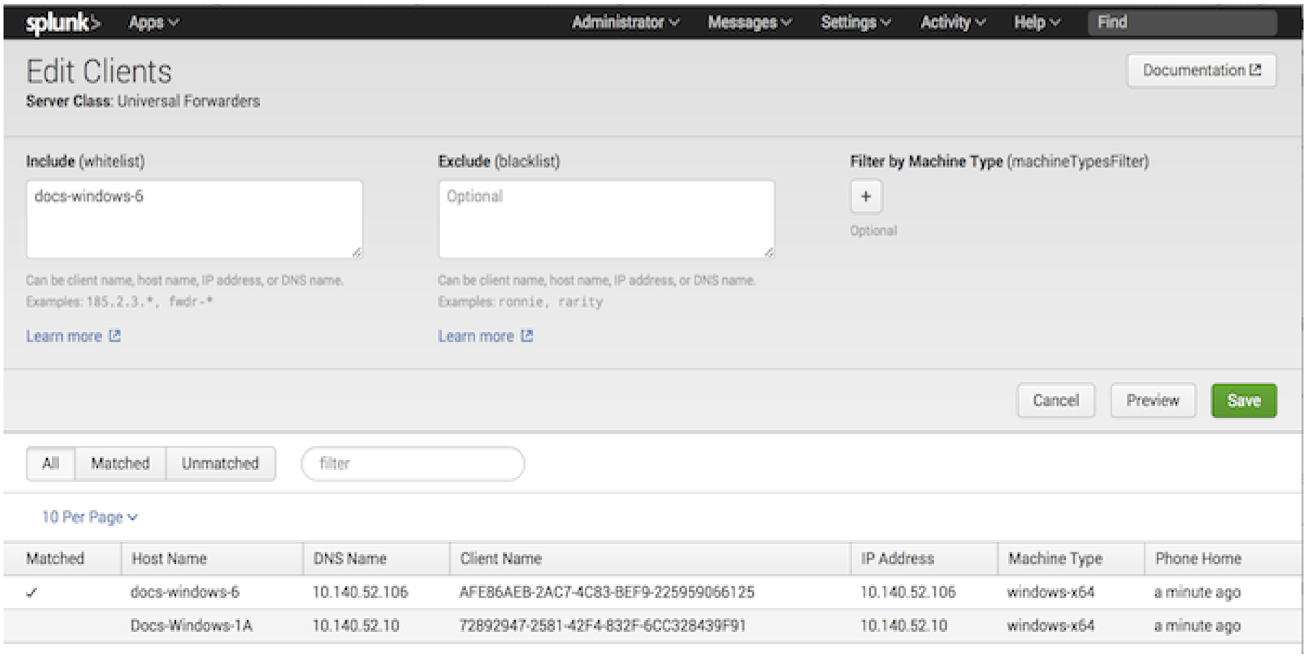
2. In the system bar, click **Settings > Forwarder Management**

3. Click the **Clients** tab.

Note: You should see the universal forwarder you installed in the previous step. If you don't, confirm that the forwarder service is active and that its configuration points to this deployment server.

4. Click the **Server Classes** tab.

5. In the server class you created earlier ("Universal Forwarders"), click **Edit**, and in the pop-up that appears, click **Edit Clients**. Splunk Enterprise loads the "Edit clients" page.



Edit Clients

Server Class: Universal Forwarders

Include (whitelist)

docs-windows-6

Can be client name, host name, IP address, or DNS name.
Examples: `185.2.3.*, fwdr-*`

Learn more

Exclude (blacklist)

Optional

Can be client name, host name, IP address, or DNS name.
Examples: `ronnie, rarity`

Learn more

Filter by Machine Type (machineTypesFilter)

+

Optional

Matched	Host Name	DNS Name	Client Name	IP Address	Machine Type	Phone Home
✓	docs-windows-6	10.140.52.106	AFE86AEB-2AC7-4C83-BEF9-225959066125	10.140.52.106	windows-x64	a minute ago
	Docs-Windows-1A	10.140.52.10	72892947-2581-42F4-832F-6CC328439F91	10.140.52.10	windows-x64	a minute ago

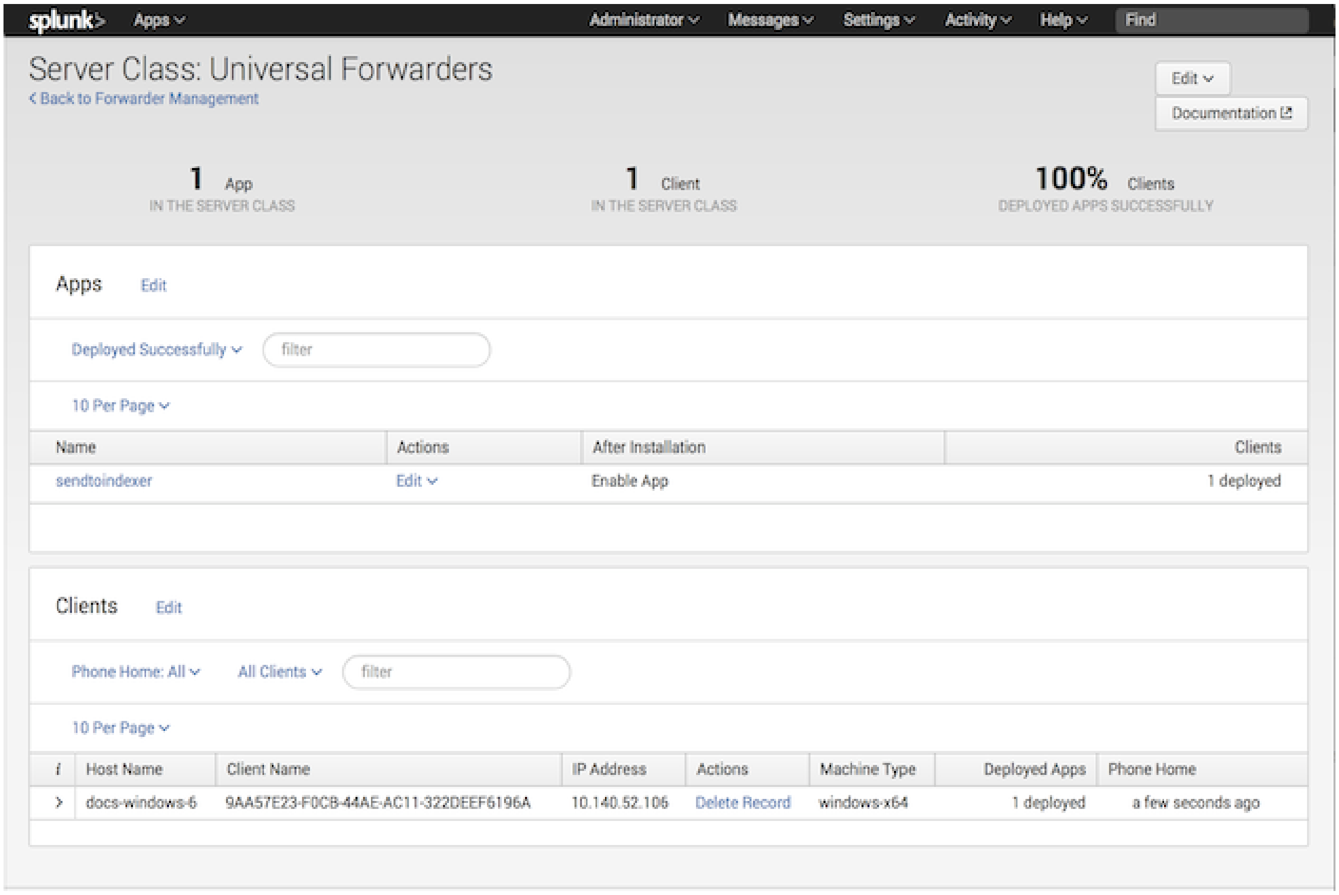
This page lists all clients that have connected to the deployment server. Those clients appear on the page below the **Include**, **Exclude**, and **Filter by Machine Type** controls at the top.

To add clients to the server class:
6. In the **Include (whitelist)** field at the top of the page, type in the host name of the deployment client.

7. Click **Preview**. Splunk Enterprise updates the list to show you which clients match the string you entered in the "Include (whitelist)" field.

8. If the results look good to you, click **Save**. Splunk Enterprise returns you to the Forwarder Management page and deploys the "send to indexer" app to the deployment client.

Review Server Class Status



Server Class: Universal Forwarders

< Back to Forwarder Management

1 App IN THE SERVER CLASS

1 Client IN THE SERVER CLASS

100% Clients DEPLOYED APPS SUCCESSFULLY

Apps Edit

Deployed Successfully filter

10 Per Page

Name	Actions	After Installation	Clients
sendtoindexer	Edit	Enable App	1 deployed

Clients Edit

Phone Home: All All Clients filter

10 Per Page

i	Host Name	Client Name	IP Address	Actions	Machine Type	Deployed Apps	Phone Home
>	docs-windows-6	9AA57E23-F0CB-44AE-AC11-322DEEF6196A	10.140.52.106	Delete Record	windows-x64	1 deployed	a few seconds ago

To confirm that the deployment server has deployed the "send to indexer" app to the deployment client, revisit the server class properties page:

1. From the Forwarder Management page, select the server class you created earlier by clicking its name in the list.

2. Review the page.

- In the upper section, you should see the "sendtoindexer" app in the list of apps within the server class. On the right side of the page, in the "Clients" column, you should see that the app has been deployed to a client.
- In the lower section, you should see the universal forwarder you installed previously. On the right side of the page, in the "Deployed Apps" column, you should see that at least one app has been deployed.

If you don't see these entries, try the following steps to troubleshoot:

- Make sure the app is in the Splunk deployment apps folder on the deployment server.

- Confirm that you have configured the deployment client with the deployment server host name or IP address and management port.
- Confirm that you can contact the deployment server on its management port from the deployment client (make sure that a firewall does not block that access.)

Splunk Add-on for Windows

The Splunk Add-on for Windows collects Windows data from Windows hosts. In the context of the Splunk App for Windows Infrastructure, the add-on collects Windows data and provides knowledge objects for the app. You should deploy the Splunk Add-on for Windows to:

- All hosts that run Active Directory Domain Services (including domain controllers and DNS servers).
- All Windows hosts from which you want Windows data.
- All indexers.
- All search heads.
- Basically, everywhere.

Downloading the Splunk Add-on for Windows

Download the app and save it to an accessible place on the deployment server:

1. In a web browser, proceed to the Splunk Add-on for Windows download page.

2. Click the download link to begin the download process.

- Make sure you download the latest version of the add-on.
- You might need to sign in with your Splunk account before the download starts.

3. When prompted, choose an accessible location on your deployment server to save the download. Do not attempt to run the download.

4. Use an archive utility such as WinZip to unarchive the file to an accessible location.

Configuring the Splunk Add-on for Windows

Before the add-on can collect Windows data, you must configure it.

1. In the location where you unarchived the download file, locate the **SPLUNK_TA_Windows** directory.

2. Inside this directory, make a subdirectory **local**.

3. Copy the **inputs.conf** file in the default subdirectory (%SPLUNK_HOME%\etc\system\(local|default)\) to the **local** directory.

4. Open the **inputs.conf** in the **local** subdirectory with a text editor, such as Notepad.

5. Enable the Windows inputs you want to get data for and delete everything else. Do this by changing the value of the **disabled** attribute in each input stanza from "1" to "0".

Note: At a minimum, enable the following sets of inputs. Do not enable the [admon] input:

Input:	Supports:
[WinEventLog://Application], [WinEventLog://Security], [WinEventLog://System],	Event Monitoring

6. Save the **inputs.conf** file in the **local** subdirectory.

Deploying the Splunk Add-on for Windows

This topic discusses deploying the Splunk Add-on for Windows to the deployment clients that you have configured to connect to the deployment server. Once you deploy the add-on, the deployment clients begin collecting Windows data and sending it to the indexer.

Deployment Apps Directory on the Deployment Server

The deployment server must be made aware of the new app. You do this by placing it in the deployment apps directory:

1. Open a command prompt on the deployment server/indexer.

2. Copy the entire Splunk Add-on for Windows folder from its current location to the deployment apps directory:

```
PS c:\> Copy-Item -Path C:\Downloads\Splunk_TA_Windows -Destination "C:\Program Files\Splunk\etc\deployment-apps\Splunk_TA_Windows" –Recurse
```

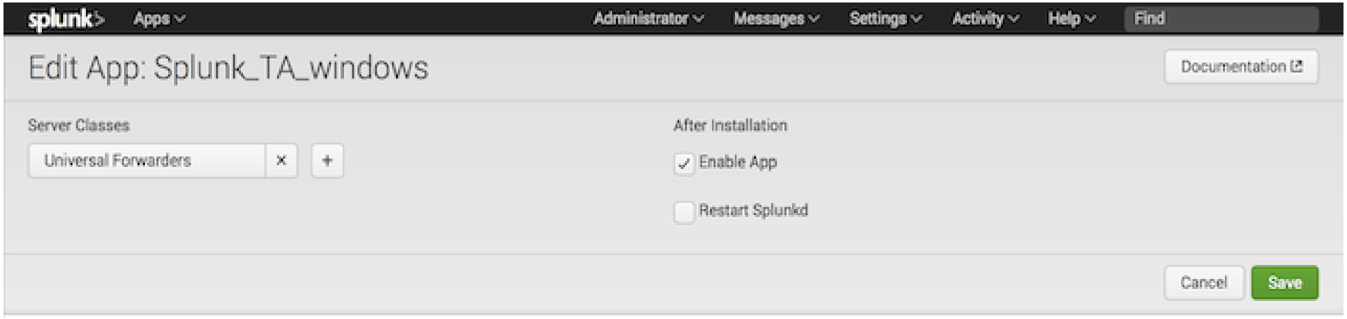
3. Tell the deployment server to reload its deployment configuration. Input credentials when prompted.

```
PS c:\> cd \Program Files\Splunk\bin
PS c:\> .\splunk reload deploy-server
```

4. From a web browser, log into Splunk Enterprise on the deployment server.

5. In the system bar, select **Settings > Forwarder Management**.

6. Click the **Apps** tab. You should see the Splunk_TA_Windows add-on in the list of apps.



Edit App: Splunk_TA_windows

Server Classes: Universal Forwarders

After Installation

☑ Enable App

□ Restart Splunkd

7. In the "Splunk_TA_Windows" add-on entry in the list, click **Edit**. Splunk Enterprise loads the "Edit App: Splunk_TA_Windows" page.

8. Click the gray "**+**" sign under "Server Classes".

9. Select the "Universal Forwarders" server class you created during initial setup. Splunk Enterprise displays the deployment clients that will receive the app in the lower half of the page. You should see the deployment client that you set up previously.

10. Place a **checkmark** next to "Restart Splunkd".

11. Click **Save**. Splunk Enterprise saves the configuration, returns you to the Forwarder Management menu, and deploys the Splunk_TA_Windows app to the deployment client.

Confirmation and Troubleshooting Windows Data Collection

This topic discusses how to confirm and troubleshoot data collection from the Splunk Add-on for Windows.

Checking the Indexer for Data

After you configure and deploy any Splunk Add-ons for Windows into your deployment client, you should check the deployment server to see that data has arrived. A few ways to check if data is being received are below.

- Check to see if you can ping between systems.
- Check to see if applicable Index is created.
- Search and Reporting app.
  - Check if it is shown as coming in within the Data Summary window.
  - Check all Indexes for the data.

        - Example: index = *

- If you do not see the deployment client host name, then there is a problem occurring between the client at the indexer. Confirm that:
    - You have properly configured receiving on the indexer.
    - You have properly configured the "send to indexer" app to forward data to the indexer.
    - No network issue exists between the deployment client and the indexer.

- Confirm that you have configured the Splunk Add-on for Windows for all inputs that you want it to collect.

- Confirm that you have placed the add-on in the deployment apps directory and reloaded the deployment server (.\splunk.exe reload deploy-server –class <class_name>.

- Restart the Spunk Forwarder service on the deployment client (restart-service –name “SplunkForwarder”.

- Confirm that the deployment client does not have errors attempting to collect the data.

- More troubleshooting steps are available in the Splunk Troubleshooting manual.

Updating Deployment Apps

At any time you can update a deployment app on the Deployment server by editing the **output.conf** file in the applicable deployment folder (%SPLUNK_HOME%\etc\deployment-apps\<app_name>\local).

Once complete, restart the Server Class containing the newly updated app. That will trigger the clients to update when they check back in.

1. Open a PowerShell prompt on the Indexer.

2. Change directory to **%SPLUNK_HOME%\bin**.

3. Type the following:

```
PS c:\program files\splunk\bin\> .\splunk.exe reload deploy-server –class <class_name>
```

Note: The Server Class name is case-sensitive.

Exporting Saved Searches

Saved searches are saved in the following locations on the server in the savedsearches.conf file.

- Public and Shared searches
    - %SPLUNK_HOME%\etc\system\(local|default)\
    - %SPLUNK_HOME%\etc\apps\(appname)\(local|default)\
- Private searches
    - %SPLUNK_HOME%\etc\users\(username)\(appname)\(local|default)\

Universal Forwarder

The Universal Forwarder is the official Splunk agent used to ship data from client systems. We will address installation of the agent on Windows and Linux systems although there are other supported platforms as well. The agents can be downloaded on the Splunk site located here.

Windows Installation (No Deployment Server)

In order to begin the data collection and forwarding process, you must install a universal forwarder on every Windows host that you want data from.

1. Confirm that your Windows host meets the minimum system requirements for a Splunk universal forwarder installation.

2. Download the appropriate universal forwarder for your version of Windows.

3. Install the universal forwarder onto the Windows host. During the installation process, follow these prompts:

- In the first dialog, check the box to accept the license agreement.
- Click **Customize Options** to customize the installation options.
- Click **Next** to advance through the "Destination Folder" dialog.
- Click **Next** to advance through the "Certificate Information" dialog.
- In the "User selection" dialog, make sure "Local System" is selected and click **Next.**
- In the "Enable Windows inputs" dialog, select the the inputs you want to collect and select **Next**.
- Click **Next** to advance through the "Deployment Server" dialog.
- In the "Specify a Receiving Indexer" dialog, the IP address of your Splunk server and then click **Next**.
- Click **Install** to accept these configurations and install the universal forwarder.

4. After installation completes, confirm that the universal forwarder service runs.

- You can check the **SplunkForwarder** service in the Services control panel, or
- In PowerShell (get-service –name “splunkforwarder”)

*nix Installation

The universal forwarder is available on Linux as a tar file, an RPM package, or a DEB package.

Install from a RedHat Package Manager (RPM) package

1. Confirm that the rpm package you want to install from is available locally on the target host and that the user that runs the forwarder can read it.

2. Use the rpm program to install RPM files. To install the Splunk RPM in the default directory /opt/splunkforwarder:

```
$ rpm -i splunkforwarder-<…>-linux-2.6-x86_64.rpm
```

3. Enable Splunk to start on boot:

```
$ /opt/splunkforwarder/bin/splunk enable boot-start
```

4. Configure Splunk forward server:

```
$ /opt/splunkforwarder/bin/splunk add forward-server :9997
```

5. Add a log file destined for forwarding – using /var/log/messages as example. You may want to do this for multiple log(s), depending on your server.

```
$ /opt/splunkforwarder/bin/splunk add monitor /var/log/messages -index main -sourcetype messages
```

6. Restart the Splunk forwarder.

```
$ service splunk restart
```

7. Verify that the forwarder is active.

```
$ /opt/splunkforwarder/bin/splunk list forward-server
```

Install from a Debian package management (DEB) file

1. Use the dpkg tool to install the Splunk DEB package. Dpkg only lets you install the DEB package into the default location, /opt/splunkforwarder.

```
$ dpkg -i splunk_package_name.deb
```

Blacklisting and Whitelisting Events

If there are specific events, you don’t care to have sent to the Splunk server, we can blacklist them in the **inputs.conf** file. This option works well when we want to see majority of the events that happen with only a few that are not important to us. It was the other way around where we only had a few events that were important to us, we would whitelist them. One or the other should be use, never both at the same time. Stanza examples of both are below.

```
[WinEventLog:Security]
disabled = false
blacklist = 5156-5157
```

```
[WinEventLog:Security]
disabled = false
whitelist = 4624, 4625, 4648
```

Note: Ranges or comma-separate event IDs or event comma-separate ranges of event IDs.

Specialized Log Ingest

DNS Logs

To get DNS logs into Splunk, we can just monitor the log file.

First, make sure DNS debugging is enable and configured. That can be accomplished easily using the below directions:

1. Open DNS.

2. Right-click on the server name and select **Properties**.

3. Click the **Debug Logging** tab.

4. Select the suitable options for you environment. I would select all options except notifications, and filter packets by IP address.

5. Take note of the log file path (most likely c:\windows\system32\dns\dns.log.

6. Click **Ok**.

7. On the Splunk server, make an index called **win_dns** (Settings > Indexes).

8. Copy the below stanza to the inputs.conf on a new or existing app.

```
[monitor:// c:\windows\system32\dns\dns.log]
disabled = false
followTail = 1
```

```
sourcetype = win_dns
index = win_dns
```

9. Reload the deployment server.

```
PS C:\Program Files\Splunk\bin> .\splunk.exe reload deploy-server –class
"<Server_Class_Name"
```

10. Restart the Splunk Forwarder service on the DNS service.

Search Premier

When you search, you are seeking to match search terms against segments of your event data. These search terms are keywords, phrases, boolean expressions, field name and value pairs, and so forth that specify which events you want to retrieve from the indexes

Keywords, Phrases, and Wildcards

Use the asterisk wildcard (*) to match an unrestricted number of characters in a string. Searching for ***** by itself means, "match all" and retrieves all events up to the maximum limit. Searching for ***** as part of a string, generates matches based on that string. For example:

- **my*** matches myhost1, myhost.ny.mydomain.com, myeventtype, etc.
- ***host** matches myhost, yourhost, etc.
- ***host*** matches host1, myhost3, yourhost27.yourdomain.com, etc

The more specific your search terms are to the events you want to retrieve, the better chance you have at matching them. For example, searching for "access denied" is always better than searching for "denied". If 90% of your events have the word ‘error’ but only 5% have the word ‘sshd’ (and the events you want to find require both of these words), include ‘sshd’ in the search to make it more efficient.

Boolean Expressions

The Splunk search processing language (SPL) supports the Boolean operators: AND, OR, and NOT. **The operators must be capitalized**.

The AND operator is always implied between terms, that is: **web error** is the same as **web AND error**.

The NOT operator only applies to the term immediately following NOT. To apply to multiple terms, you must enclose the terms in parenthesis.

Splunk software evaluates Boolean expressions in the following order:

1. Expressions within parentheses.

2. **NOT** clauses.

3. **OR** clauses.

4. **AND** clauses.

Splunk Software Expressions Processing

Consider the following search.

A=1 AND B=2 OR C=3

When you specify values without parenthesis, this search is processed as

A=1 AND (B=2 OR C=3)

Here is another example.

Error NOT 403 OR 404

Without parenthesis, this search is processed as error **NOT = 403 OR error = 404**

You can use parentheses to group Boolean expressions. For example:

Error NOT (403 OR 404)

(A=1 AND B=2) OR C=3

Note: Inclusion is generally better than exclusion. Searching for "access denied" will yield faster results than NOT "access granted".

Comparison Operator Usage

You can use comparison operators to match a specific value or a range of field values.

Operator	Example	Result
=	Field = foo	Multivalued field values that match exactly “foo”.
!=	Field != foo	Multivalued field values that do not match “foo”.

<	Field < X	Numerical field values that are less than X.
>	Field > X	Numerical field values that are greater than X.
<=	Field <= X	Numerical field values that are less than or equal to X.
=>	Field => X	Numerical field values that are equal to or greater than X.

For example, to find events that have a delay field that is greater than 10:

Delay > 10

Search Examples

Below are a few examples. On my github (www.github.com/wiredpulse) are custom searches that will provide additional examples for you.

- Looking for all data in the Splunk instance
  Index = *
- Looking for data concerning a system named “Win7-1” in any index
  Index = * Host = “win7-1”
- Looking for data concerning a system named “Win7-1” in a specific index
  Index = “win_security” host = “win7-1”
- Looking for an Event Code with a specific sub status code
  EventCode = 4625 (Sub_Status=”0x000072 OR Sub_Status=”0xC000072”)

PowerShell Scripts, Custom Searches, and Dashboards

On my github (www.github.com/wiredpulse), I currently have Splunk PowerShell scripts, searches and dashboards. As I develop more, I will place I will upload them there as well.