

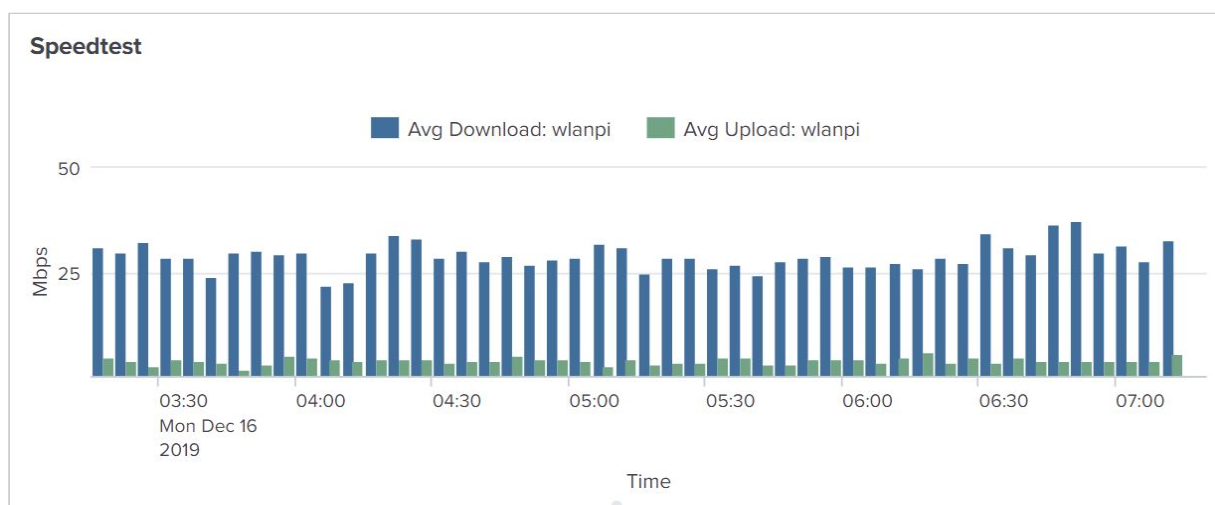
Wiperf - Splunk Build

1 Background	2
2 Installation	4
3 Connectivity Planning	4
3.1 Results Data Over Wireless	6
3.2 Results data over Ethernet	7
3.3 Results data over Zerotier/wireless	8
4 Basic Splunk Build	10
4.1 Download	10
4.2 Installation	12
4.2.1 Linux (Debian)	12
4.2.1.1 Starting Splunk	13
4.2.1.2 Automating Startup	14
4.2.2 Mac OS	15
4.2.3 Windows	19
4.2.4 Firewalls	21
5 Customizing Splunk	22
5.1 Configure Data Input To Splunk	22
5.1.1 Log In To Splunk	22
5.1.2 Configure HTTP Event Collector Global Options	22
5.1.3 Create a HEC Token	25
5.1.4 Perform a Test Search	29
5.2 Create a Dashboard	30

1 Background

The WLANPi Wiperf mode allows the WLANPi to become a standalone probe that will join a wireless network and run a series of performance tests that provide indications about how well its connection is performing. This data may be used, in conjunction with other data sources, to gain an understanding of the health of the wireless environment.

For more information about Wiperf on the WLANPi, please visit the project GitHub page at : <https://github.com/wifinigel/wiperf>



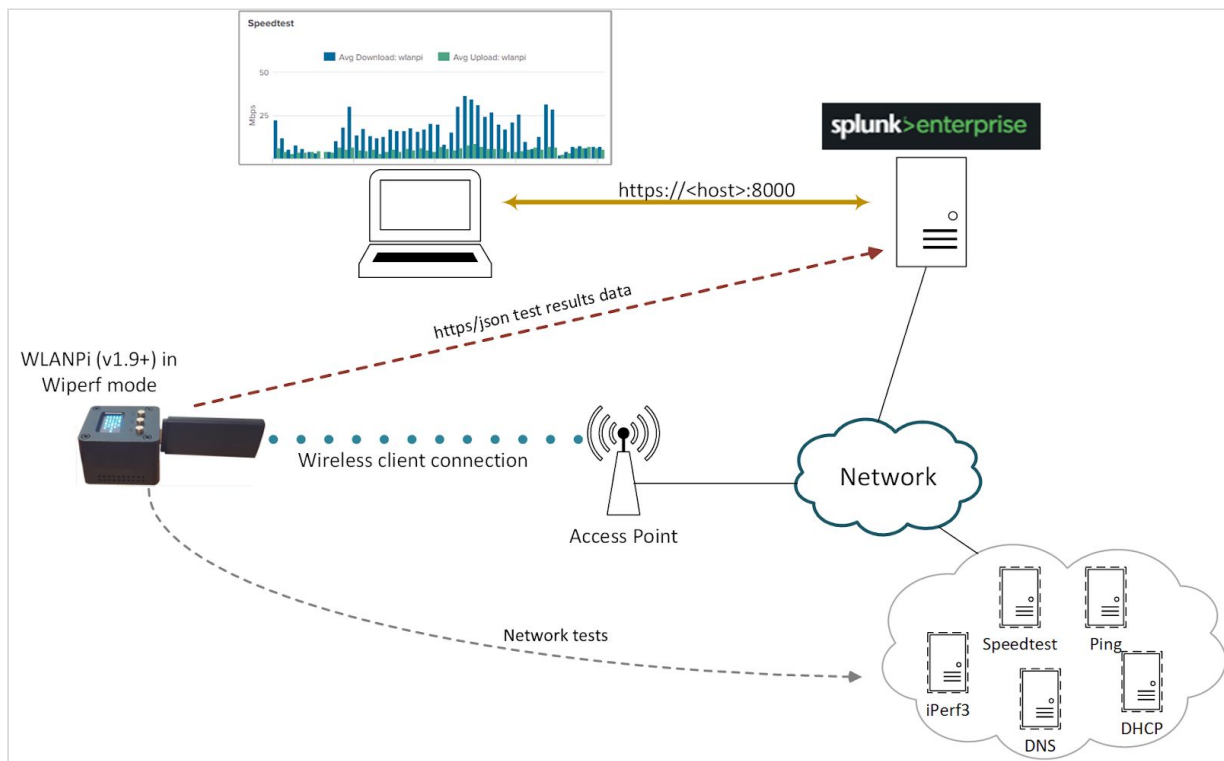
The performance tests that can be run include:

- Speedtest
- Ping (to multiple destinations)
- Iperf3 TCP test
- Iperf3 UDP test
- DNS lookup tests (multiple name queries)
- DHCP renew test

To visualize the performance data gathered by the WLANPi, a reporting server is required to receive the data and visualize it using a reporting package. In this paper we look at how WLANPi data can be sent to a Splunk server and a report created to visualize that data.

Splunk is a powerful data analytics tool that can take data from a variety of sources and allow it to be analyzed and visualized. In the case of the WLANPi, we generate data from the performance tests it runs and then send it over an https connection to a Splunk server in a JSON data format.

The interaction of all components is summarized below:



The operation is summarized as follows:

- The WLANPi is configured as a wireless network client and joins the network under test
- The WLANPi regularly runs a series of configurable network tests (controlled by a cron job within the WLANPi)
- After each test, the results data is sent over an https connection from the WLANPi to a Splunk server
- The Splunk server analyzes the data and makes it available via a “dashboard”
- A user who needs to view the performance data from the WLANPi logs in to the reporting GUI of the Splunk server and reviews the performance dashboard

2 Installation

To collect and view the test results data, an instance of Splunk is required. Splunk is a very flexible data collection and reporting package that can take data sent by the WLANPi and present it in a very nice report format. Splunk can be installed on a wide variety of platforms that can be viewed at : https://www.splunk.com/en_us/download/splunk-enterprise.html

This guide does not cover all installation details of the software package, these may be obtained when downloading and installing the software. Note that a free account sign-up is required when downloading the software from the link listed above.

To install Splunk and use it with a handful of probes, a modest server may be built (e.g. I use a low-end Intel NUC), so for testing purposes, don't get too hung up on sourcing a high end server.

The product being installed is Splunk Enterprise. This is a paid-for product, but it has a free-tier for low data volumes (500Mbytes per day). Install initially with all the licensing defaults and then drop back to the free-tier once the eval licence expires a few weeks later. The free tier is plenty for the low volume rates that the WLANPi generates when deploying probes at small-scale.

3 Connectivity Planning

One area to consider is connectivity between the WLANPi and the Splunk instance. The WLANPi needs to be able to access the Splunk server to send its data. If the WLANPi probe is being deployed on a wireless network, how is the performance data generated going to get back to the Splunk server?

If the probe is being deployed on a customer network to perform temporary monitoring, it will obviously join the wireless network under test. But how is the WLANPi going to send its data to

the Splunk server ? Many environments may not be comfortable with hooking up the WLANPi to their wired network, hence (potentially) bridging wired and wireless networks. Therefore, in many instances an alternative is required (e.g. send the results data over the wireless network itself out to the Internet to a cloud instance or via a VPN solution such as [Zerotier](#).

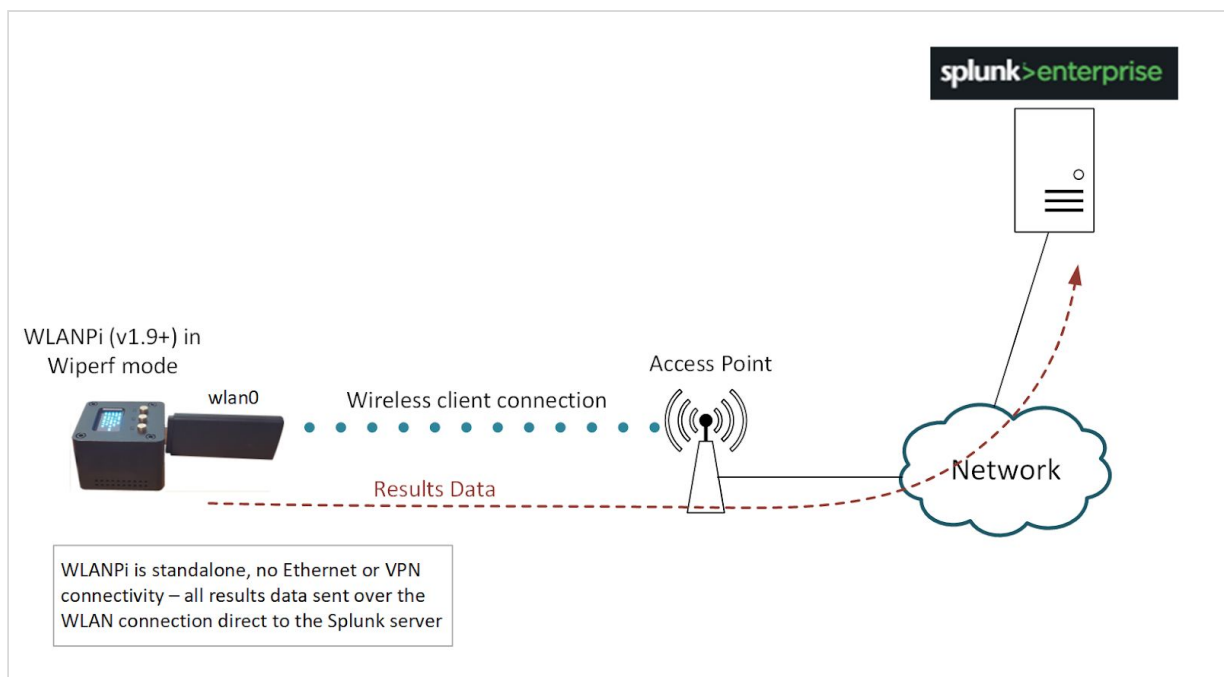
Three topology deployment options are supported:

1. Results data over wireless
2. Results data over Ethernet
3. Results data over VPN/wireless

The method used is configured on the WLANPi probe prior to flipping it in to Wiperf mode by configuring its config.ini file. It is important to understand the (viable) connectivity path prior to deploying both the probe and the Splunk server.

The 3 connectivity options are discussed below.

3.1 Results Data Over Wireless

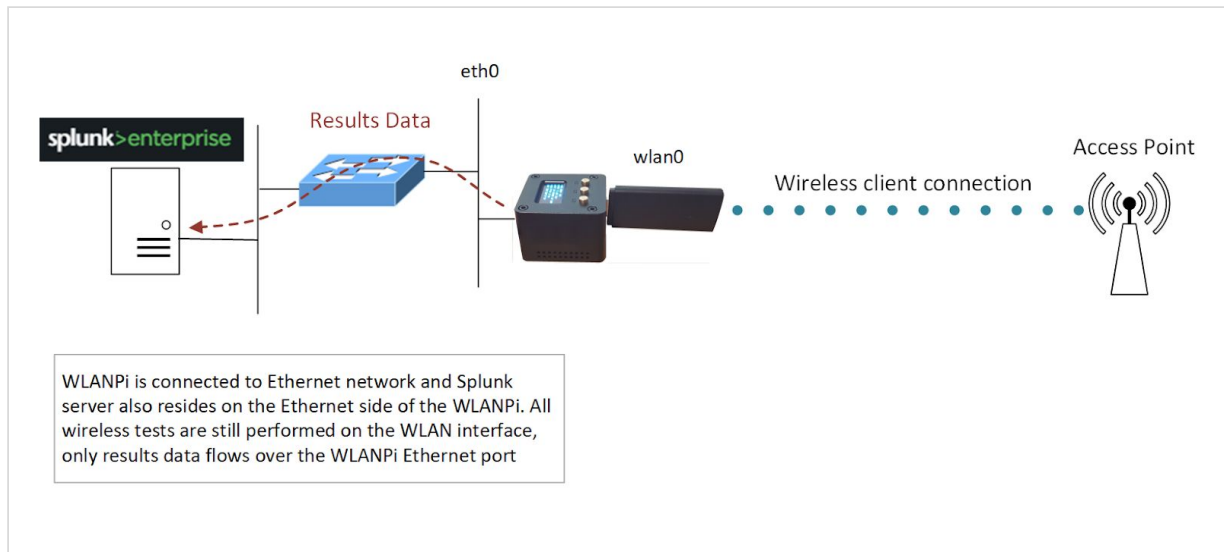


In this topology the WLANPi is configured to join an SSID that has the Splunk server accessible via its WLAN interface. Typically, the Splunk server will reside in a cloud or perhaps on a publicly accessible VPS. The WLANPi will continually run the performance tests over the wireless connection and then upload the results directly to the Splunk server over the WLAN connection.

Config.ini settings:

```
g _ f:   a 0
da a_   : < b c IP add e   f S       e e >
```

3.2 Results data over Ethernet



If the Splunk server is being run on the inside of a network environment, it may be preferable to return results data via the Ethernet port of the WLANPi. This topology also has the advantage of results data not being impacted if there are wireless connectivity issues on the WLANPi WLAN connection. To achieve the correct traffic flow, a static route for management traffic is injected into the route table of the WLANPi to force results data over the Ethernet port. Note that the Ethernet port must be connected and up when switching the WLANPi into Wiperf mode for routing to work correctly.

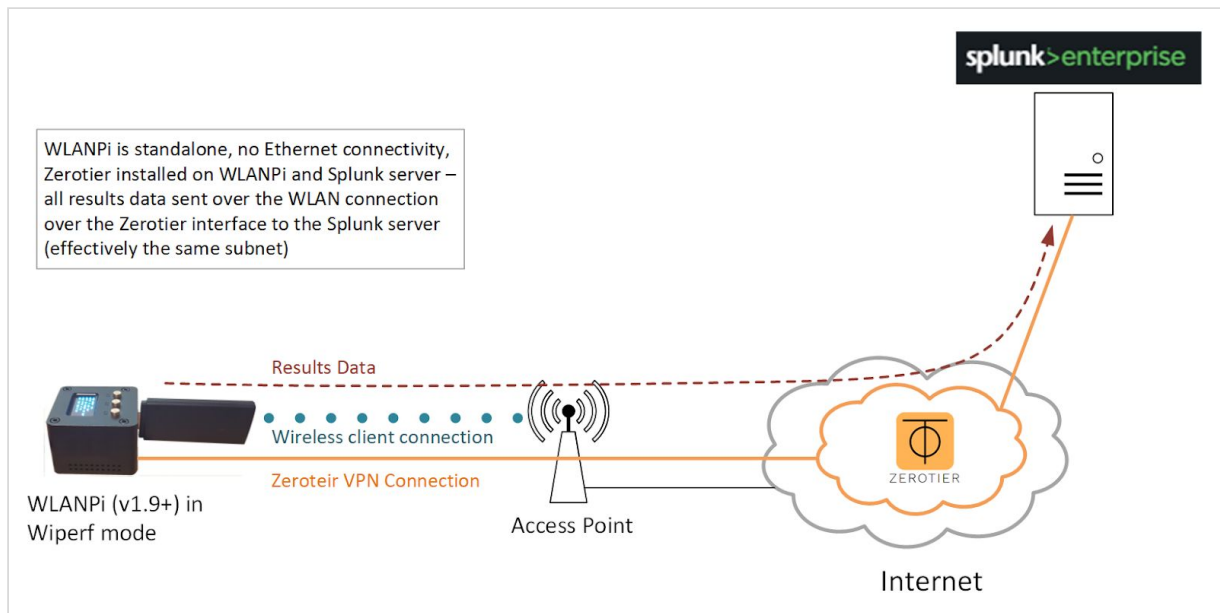
Config.ini settings:

```
g _ f: e 0
da a_ : <IP add e f S e e >
```

Security notes:

- to prevent traffic leaking between the WLAN and Ethernet interfaces of the WLANPi, IP forwarding is not enabled on the WANPi
- In Wiperf mode, the WLANPi internal firewall allows only connectivity over port 22 incoming over the ethernet and wlan interfaces - all other ports are blocked

3.3 Results data over Zerotier/wireless



A very simple way of getting the WLANPi talking with your Splunk server is to use the Zerotier service to create a virtual network. In summary, both the Splunk server and WLANPi have the Zerotier client installed. Both are then added to your Zerotier dashboard (by you) and they start talking! Under the hood, both devices have a new virtual network interface created and they connect to the Zerotier cloud-based network service so that they can communicate on the same VLAN in the cloud. As they are on the same subnet from a networking perspective, there are no routing issues to worry about to get results data from the WLANPi to the Splunk server.

Zerotier has a free subscription tier which allows up to 100 devices to be hooked up without having to pay any fees, It's very easy to use and get going, plus your Splunk server can be anywhere! (e.g. on your laptop at home). Both devices need access to the Internet for this solution to work.

You can sign up for free, create a virtual network and then just add the IDs that are created by the Splunk server and WLANPi when the client is installed.

Seriously, give it a go...it's quicker to try it than me explaining it here:

<https://www.zerotier.com/>

Config.ini settings:

```
g _ f:
da a_ : <IP address of Server to connect to>
```

To install Zerotier on the WLANPi (or an Ubuntu server), enter the following:

```
c - :// a . e . c d ba
d e e -c <network number from your Zerotier dashboard>
d e e -c a

# T e e a a a e da e:
d a e e e e - e
```

4 Basic Splunk Build

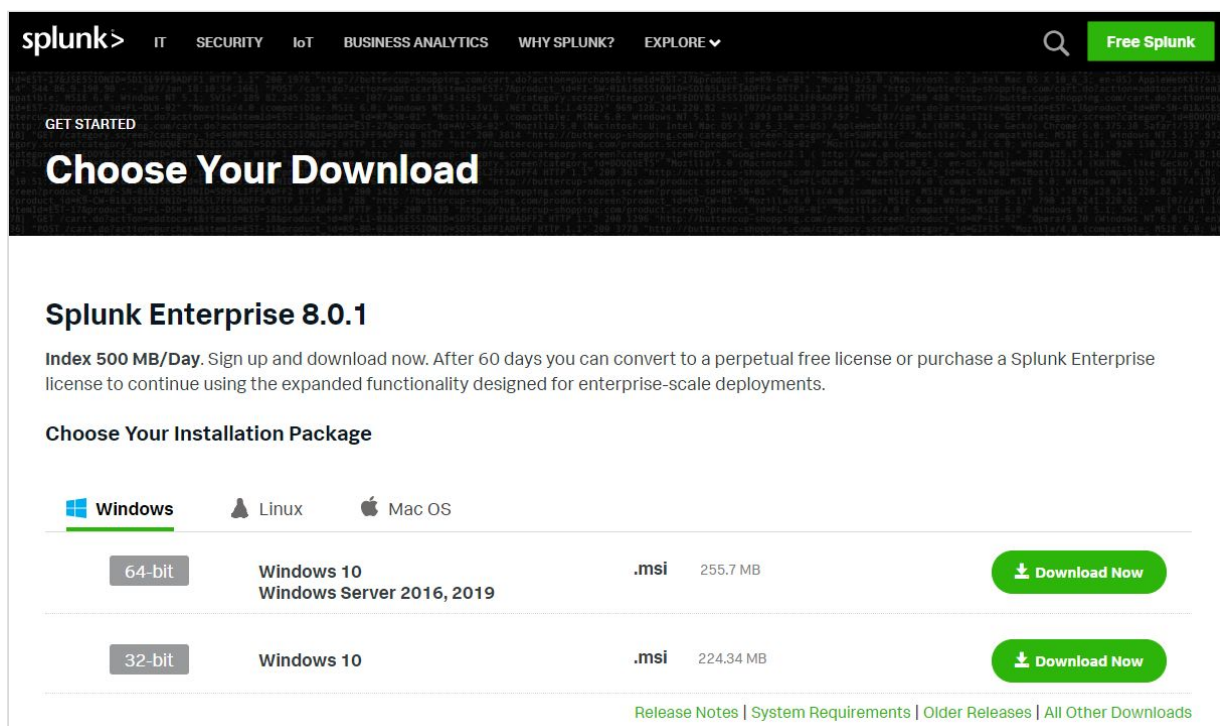
Here are the basic steps you will need to install Splunk once you have built your Splunk server hardware/instance.

4.1 Download

Get along to the Splunk web site and sign up for an account if you don't already have one:

https://www.splunk.com/en_us/download/splunk-enterprise.html

Once you're logged in to the Splunk site, you'll have a number of OS options, so go ahead and choose your OS option. There are options for Windows, Linux & Mac OS:



splunk> IT SECURITY IoT BUSINESS ANALYTICS WHY SPLUNK? EXPLORE ▼ Free Splunk

GET STARTED

Choose Your Download

Splunk Enterprise 8.0.1

Index 500 MB/Day. Sign up and download now. After 60 days you can convert to a perpetual free license or purchase a Splunk Enterprise license to continue using the expanded functionality designed for enterprise-scale deployments.

Choose Your Installation Package

	Windows	Linux	Mac OS
64-bit	Windows 10 Windows Server 2016, 2019		
32-bit	Windows 10		

[Release Notes](#) | [System Requirements](#) | [Older Releases](#) | [All Other Downloads](#)

splunk> IT SECURITY IoT BUSINESS ANALYTICS WHY SPLUNK? EXPLORE

GET STARTED

Choose Your Download

Splunk Enterprise 8.0.1

Index 500 MB/Day. Sign up and download now. After 60 days you can convert to a perpetual free license or purchase a Splunk Enterprise license to continue using the expanded functionality designed for enterprise-scale deployments.

Choose Your Installation Package

Windows **Linux** Mac OS

64-bit

Package	Size	Action	
2.6+, 3.x+ or 4.x+ kernel Linux distributions	.deb	337.77 MB	Download Now
	.tgz	447.6 MB	Download Now
	.rpm	447.81 MB	Download Now

[Release Notes](#) | [System Requirements](#) | [Older Releases](#) | [All Other Downloads](#)

splunk> IT SECURITY IoT BUSINESS ANALYTICS WHY SPLUNK? EXPLORE

GET STARTED

Choose Your Download

Splunk Enterprise 8.0.1

Index 500 MB/Day. Sign up and download now. After 60 days you can convert to a perpetual free license or purchase a Splunk Enterprise license to continue using the expanded functionality designed for enterprise-scale deployments.

Choose Your Installation Package

Windows Linux **Mac OS**

Intel

Package	Size	Action	
OSX 10.13 OSX 10.14	.tgz	363.56 MB	Download Now
	.dmg	370.71 MB	Download Now

[Release Notes](#) | [System Requirements](#) | [Older Releases](#) | [All Other Downloads](#)

Once you have hit the download button, the Splunk Enterprise software chosen will start to download to your local machine, ready for installation.

It's worth checking the download page to see if there are further download options. If you check the graphic below, you can see there is a "Download via Command Line (wget)" option, which is a much easier way to get the code directly on to your server. The options you will see here will vary between OS selections.



4.2 Installation

Once the software is downloaded, follow the instructions that are appropriate for your OS in the Splunk installation manual (you can look for the latest guides via Google, but at the time of writing it was this manual):

<https://docs.splunk.com/Documentation/Splunk/8.0.1/Installation/Chooseyourplatform>

4.2.1 Linux (Debian)

Note that while compiling this guide I was performing a build on a Debian Linux platform (Ubuntu in this case) so have provided an overview of the required steps and included them in green dialog boxes, like the one shown below, throughout this section. Note that other flavours of Linux are likely to be similar, but you must consult the installation guide to ensure you complete all installation steps correctly:

- <https://docs.splunk.com/Documentation/Splunk/8.0.1/Installation/InstallonLinux>

For a Debian Linux server use the following command to install the downloaded file:

```
# d g - -8.0.1-6db836e2fb9e- -2.6-a d64.deb
```

4.2.1.1 Starting Splunk

Go to the 'Next Steps' section of the installation manual and find out how to start Splunk for the first time and create admin credentials.

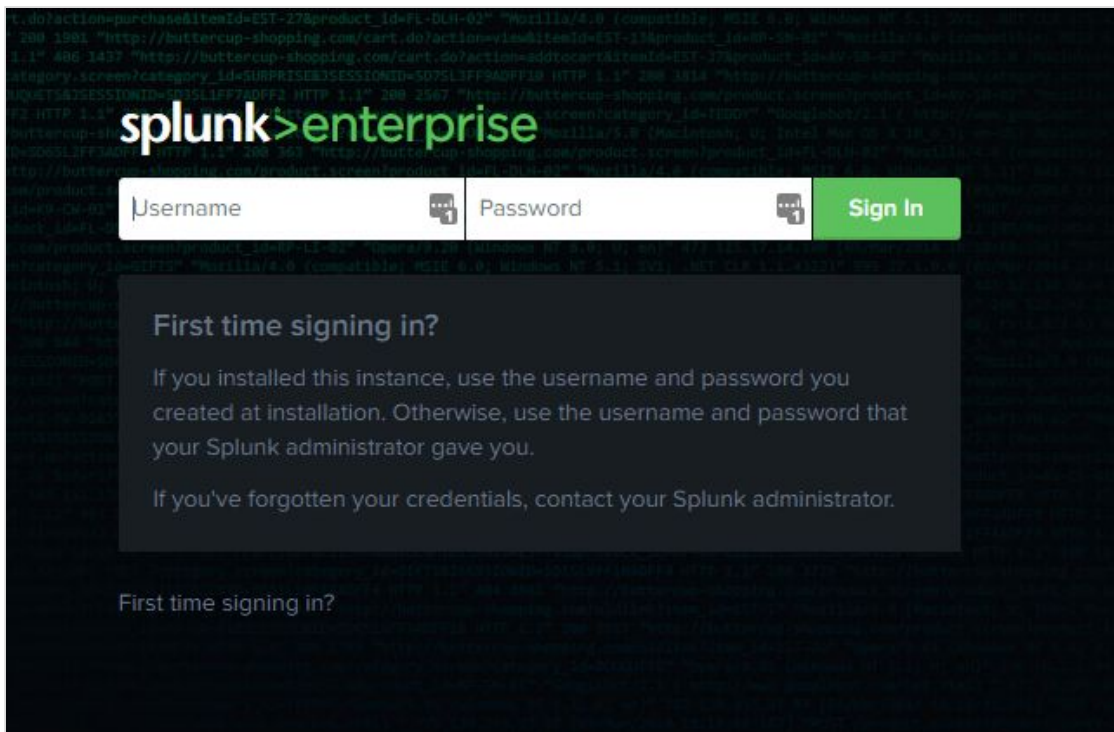
On a Debian Linux server, enter the following commands:

```
# cd / / /b
# d . / a
```

Accept the license agreement and enter a Splunk admin name and password to create an administrator account for your Splunk application.

The web interface for the Splunk server will now be started and the URL of the web GUI shown in the startup dialogs. You may now login to the Splunk web GUI using the admin credential created above. The web GUI is accessed at the URL:

http://<Splunk_server_IP>:8000



4.2.1.2 Automating Startup

Finally, ensure you follow the instructions in the installation manual to enable the Splunk application to auto start if the server is rebooted.

On a Debian Linux server, enter the following:

```
d / / /b / e ab e b - a
```

Basic server installation for Linux is now complete.

Visit the “Customizing Splunk” section of this document to setup Splunk to receive data and report on the WLANPi

4.2.2 Mac OS

Installation on Mac OS is very straightforward. The full installation guide can be obtained from the link below:

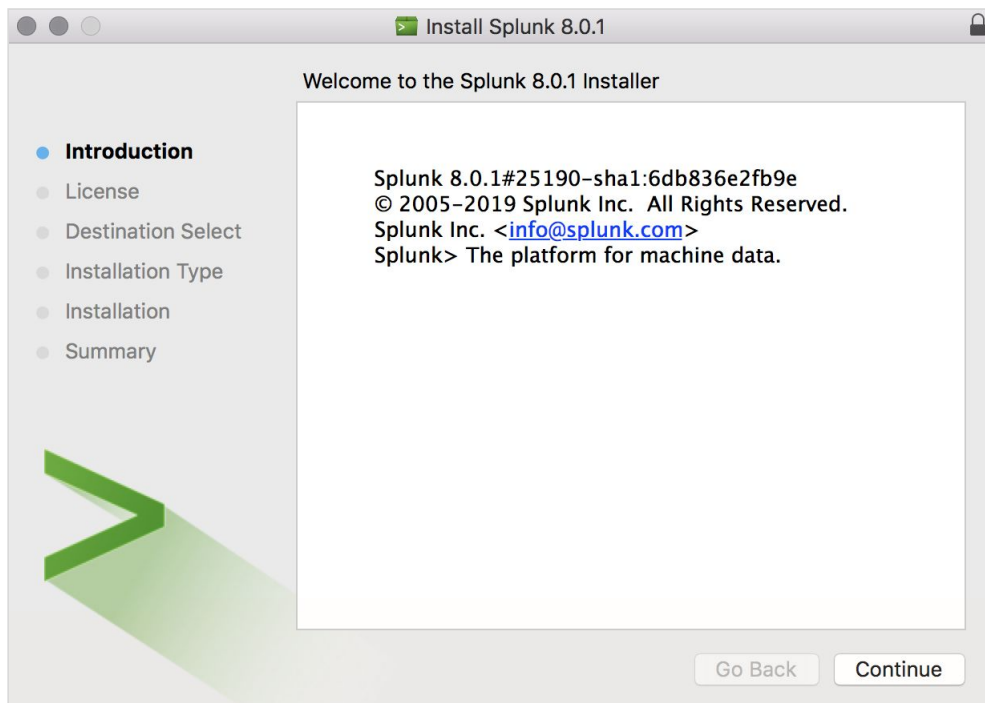
<https://docs.splunk.com/Documentation/Splunk/8.0.1/Installation/InstallonMacOS>

In summary, if you are used to downloading DMG files and installing them as applications on your Mac machine, you will find the process very straightforward.

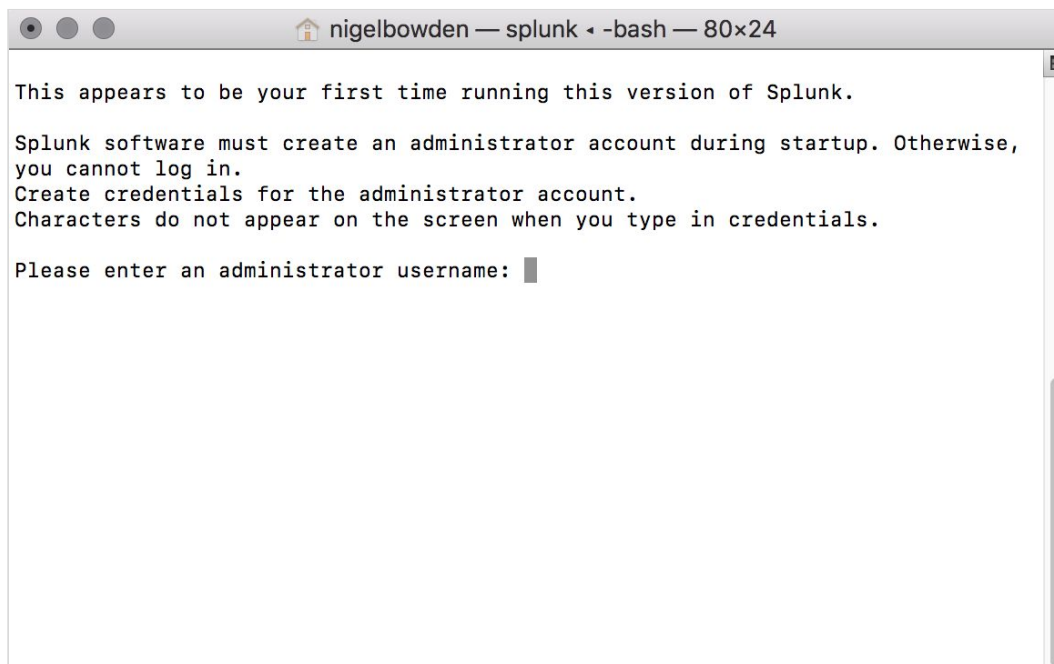
Once the DMG file has been downloaded, go into Finder and double click the downloaded dmg file to start the installer:



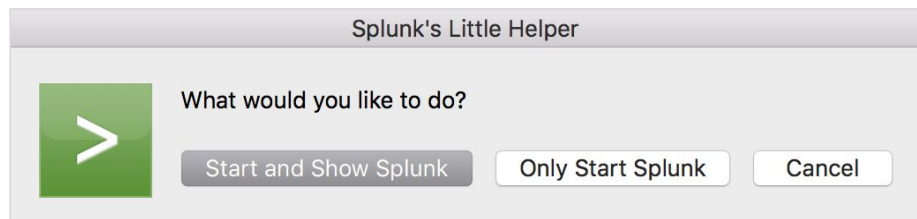
Hit continue to walk through the installation options until you see the “Install” button.



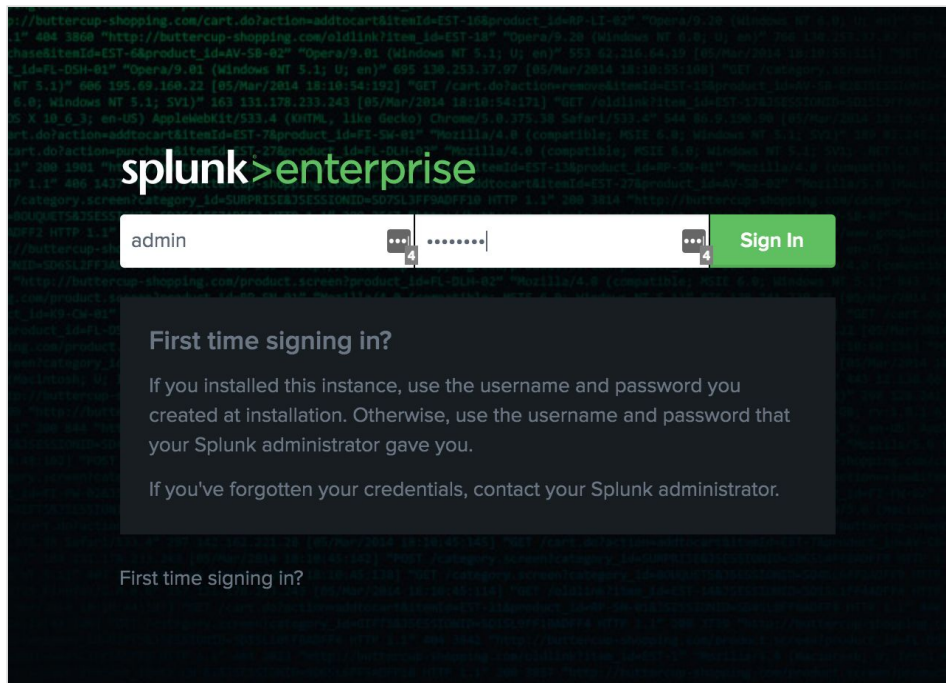
During the installation you will be prompted to enter the credentials you will use to login to the application:



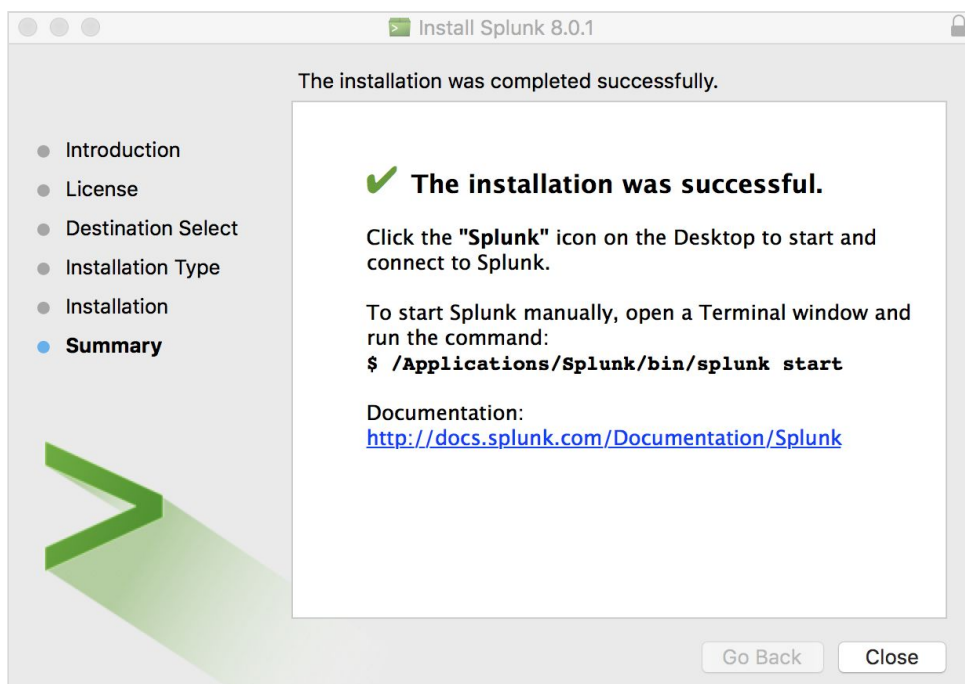
Once installation of all required files is complete, the following helper will pop up to fire up the Splunk server and start your browser to direct you to the login page (Hit “Start and Show Splunk”)



Login to the Splunk application using the credentials created during the installation process:



Finally, an "installation success" dialog panel will be shown once all steps are complete:



Note that there are no further steps required for Mac OS to start services or ensure services start on reboot - all processes are automated by the installation process.

If a CLI install is required or services need to be controlled via CLI, then visit the Splunk installation manual for Mac OS and view the CLI options and the next steps section:

- <https://docs.splunk.com/Documentation/Splunk/8.0.1/Installation/InstallonMacOS>

Basic server installation for Mac OS is now complete.

Visit the “Customizing Splunk” section of this document to setup Splunk to receive data and report on the WLANPi

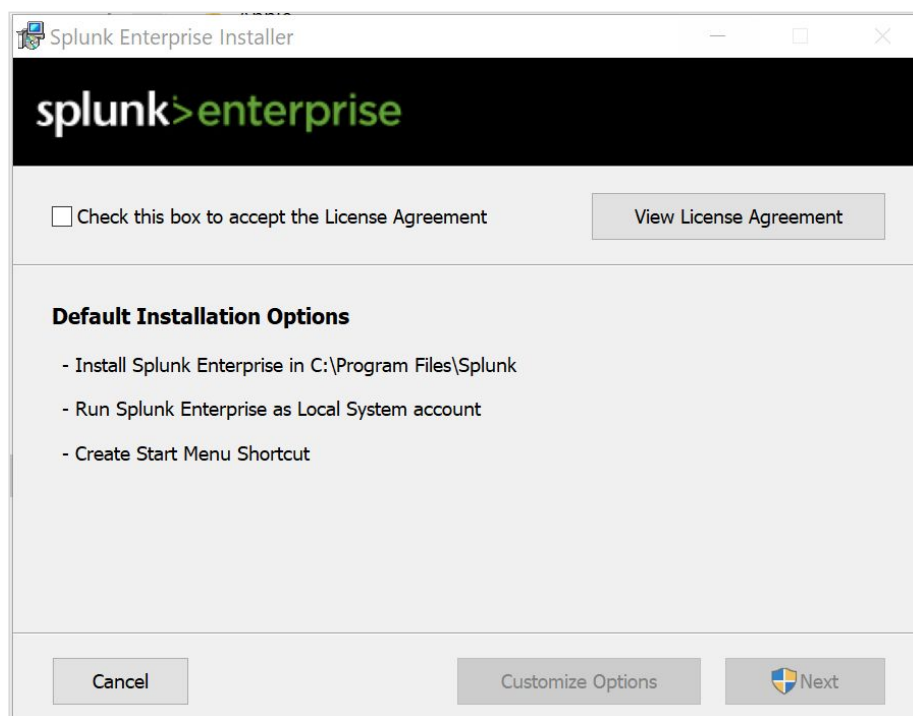
4.2.3 Windows

Installation on Windows is very straightforward. The full installation guide can be obtained from the link below:

<https://docs.splunk.com/Documentation/Splunk/8.0.1/Installation/InstallonWindows>

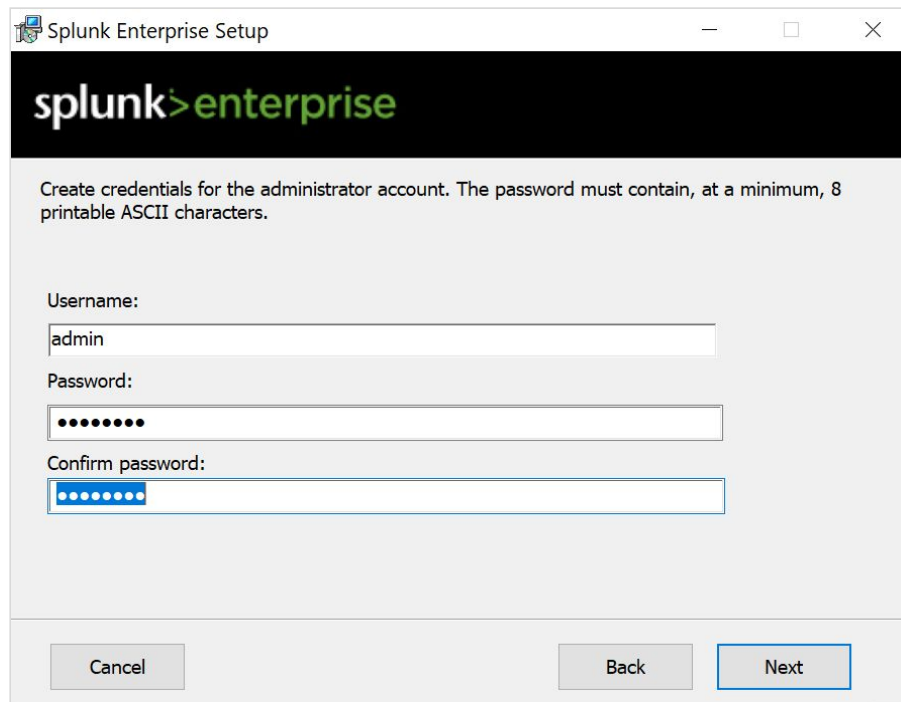
In summary, if you are used to downloading EXE or MSI files and installing them as applications on your Windows machine, you will find the process very straightforward.

Once the MSI file has been downloaded, go to your download folder and double click the downloaded MSI file to start the installer:



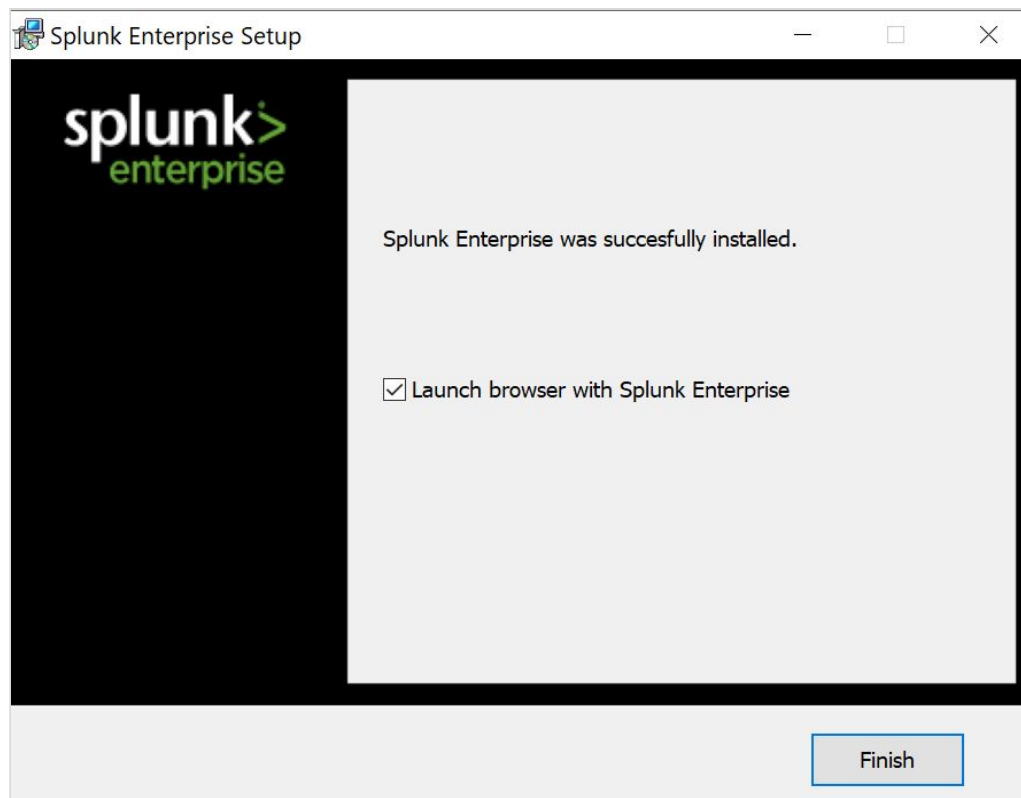
A wizard will open and a traditional next -> next -> next workflow with installation options is presented.

During the installation process, a dialog to setup access credentials for the Splunk application is presented. These credentials are required to login to the application admin GUI and configure all required data collection options:



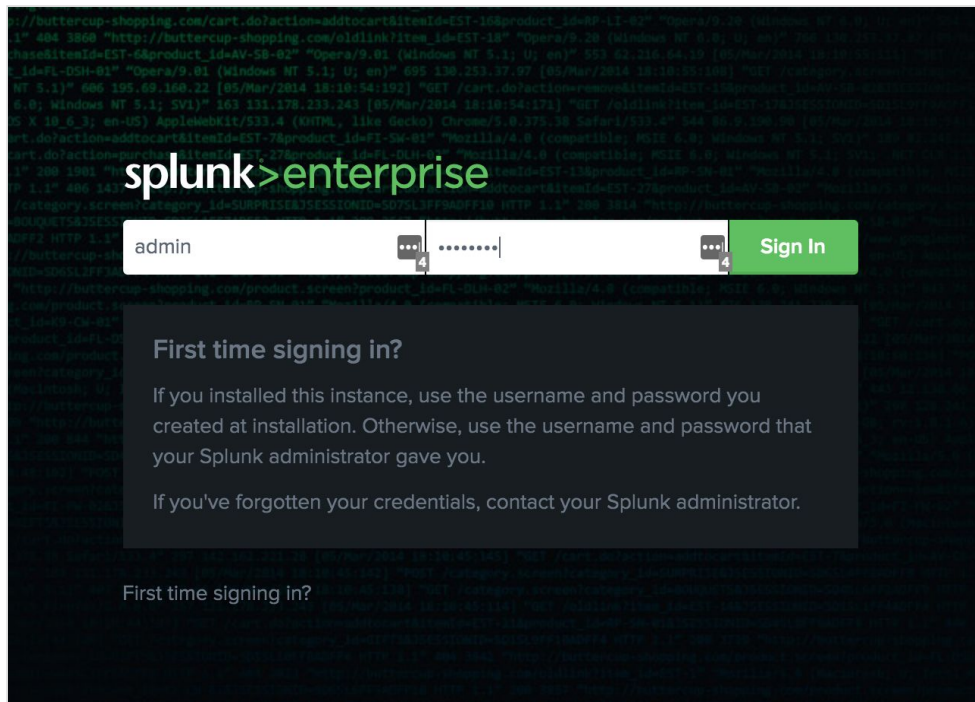
The screenshot shows the 'Splunk Enterprise Setup' window. The title bar includes the window icon, the text 'Splunk Enterprise Setup', and standard minimize, maximize, and close buttons. The main content area has a black header with the 'splunk>enterprise' logo. Below the header, a message states: 'Create credentials for the administrator account. The password must contain, at a minimum, 8 printable ASCII characters.' There are three input fields: 'Username:' with the text 'admin', 'Password:' with eight dots, and 'Confirm password:' with eight dots. At the bottom, there are three buttons: 'Cancel', 'Back', and 'Next'.

Several panels will be shown as various files and components are installed. After around 5 minutes, the installation success panel is shown:



The screenshot shows the 'Splunk Enterprise Setup' window at the success stage. The title bar is the same as the previous window. The main content area has a black header with the 'splunk>enterprise' logo. The central text reads: 'Splunk Enterprise was succesfully installed.' Below this, there is a checkbox labeled 'Launch browser with Splunk Enterprise' which is checked. At the bottom right, there is a 'Finish' button.

When “Finish” is pressed on the final panel, the local browser is launched and the login to the Splunk application is presented:



Note that there are no further steps required for Windows to start services or ensure services start on reboot - all processes are automated by the installation process.

If more advanced installation or support options are required, then visit the Splunk installation manual for Windows and visit the next steps section:

- <https://docs.splunk.com/Documentation/Splunk/8.0.1/Installation/InstallonWindows>

Basic server installation for Windows is now complete.

Visit the “Customizing Splunk” section of this document to setup Splunk to receive data and report on the WLANPi

4.2.4 Firewalls

5 Customizing Splunk

Now that we have a Splunk server setup, we need to customize it to report our WLANPi data. The steps required are all via the Splunk web GUI and are the same for all OS flavours.

5.1 Configure Data Input To Splunk

We need to tell Splunk how we'll be sending the data from our WLANPi probe in to Splunk. We need to configure a data input that will prepare Splunk to receive the data and generate an authorization key to be used by the WLANPi when sending data.

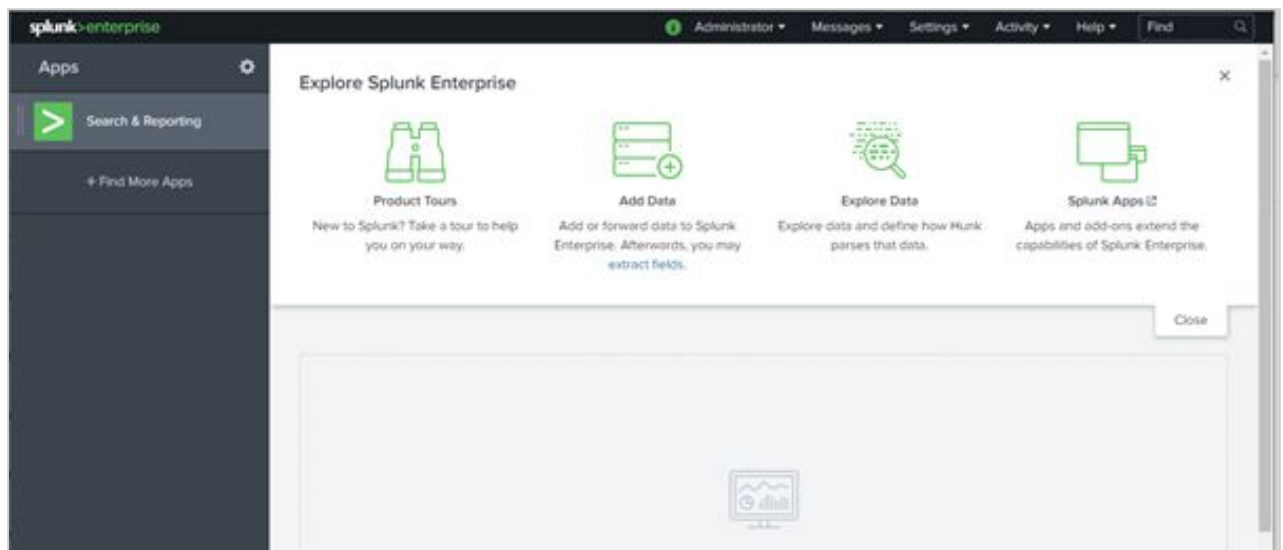
5.1.1 Log In To Splunk

The first step is to login to Splunk using the credentials created during the Splunk install. The URL to use is:

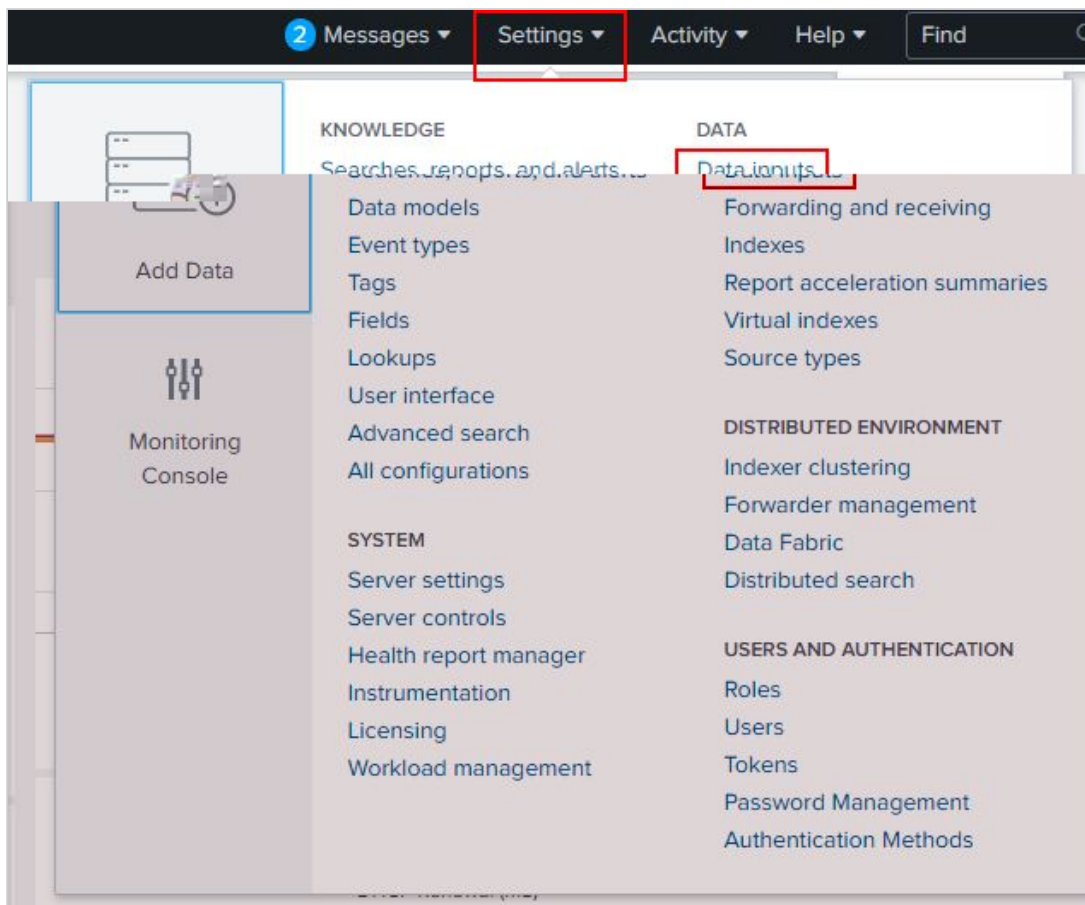
```
http://<Splunk_server_IP>:8000
```

5.1.2 Configure HTTP Event Collector Global Options

After login, the following page will be seen



Follow the “Settings > Data > Data Inputs” menu options :

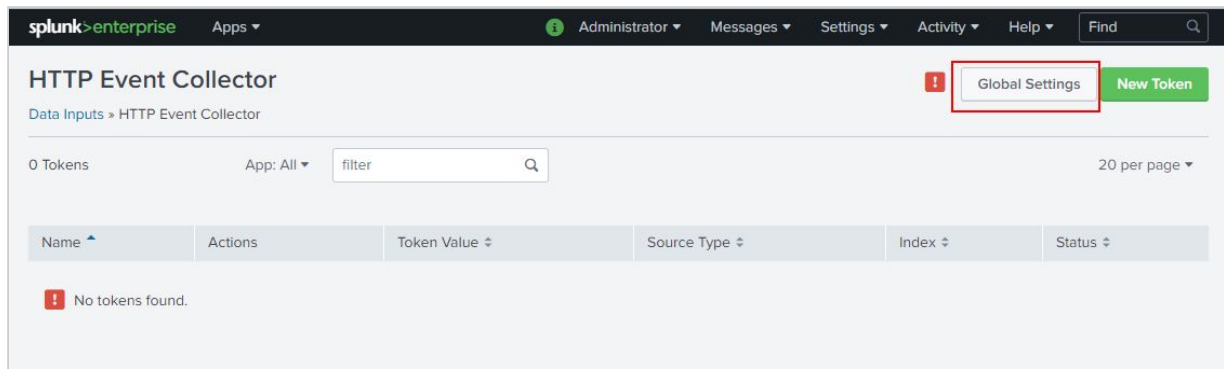


Click on the HTTP Event Collector link in the Data Inputs page shown:

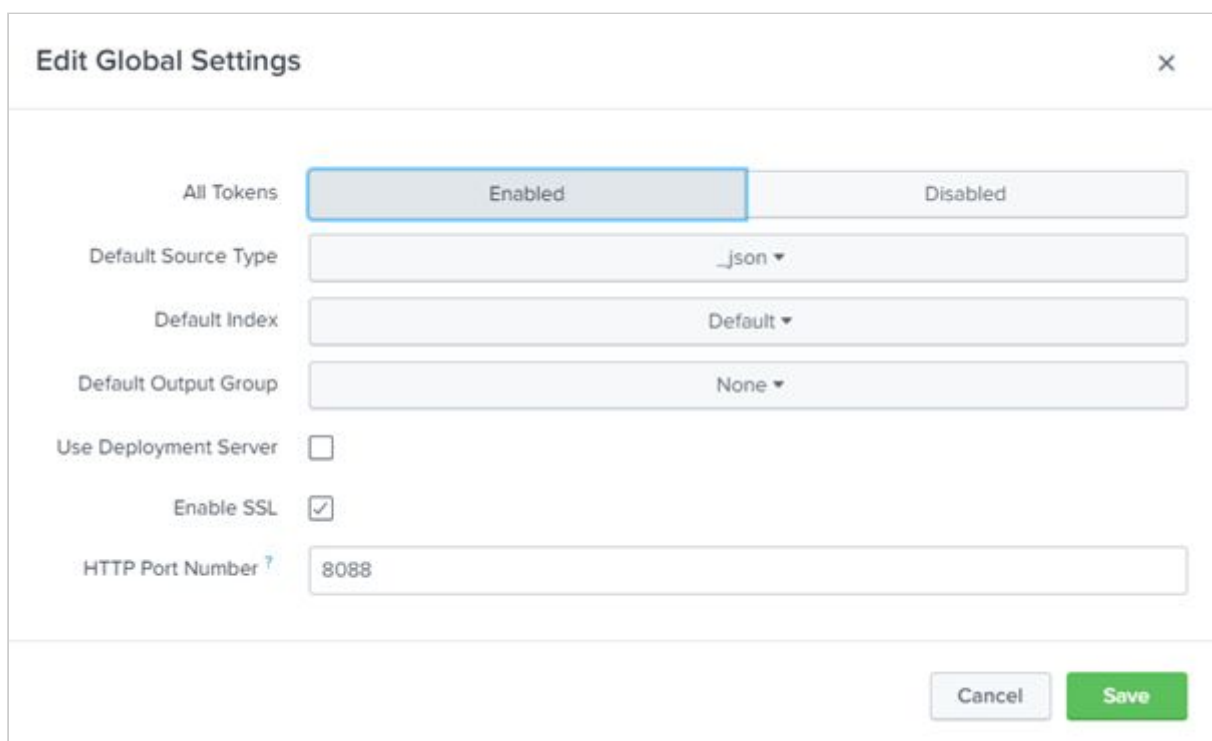
Data inputs
Set up data inputs from files and directories, network ports, and scripted inputs. If you want to set up forwarding and receiving between two Splunk instances, go to [Forwarding and receiving](#).

Local inputs

Type	Inputs	Actions
Files & Directories Index a local file or monitor an entire directory.	9	+ Add new
HTTP Event Collector Receive data over HTTP or HTTPS.	0	+ Add new
TCP Listen on a TCP port for incoming data, e.g. syslog.	0	+ Add new
UDP Listen on a UDP port for incoming data, e.g. syslog.	0	+ Add new
Scripts Run custom scripts to collect or generate more data.	5	+ Add new



Click on the “Global Settings” button as indicated in the graphic above to reveal the global configuration panel for the HTTP Event Collector:

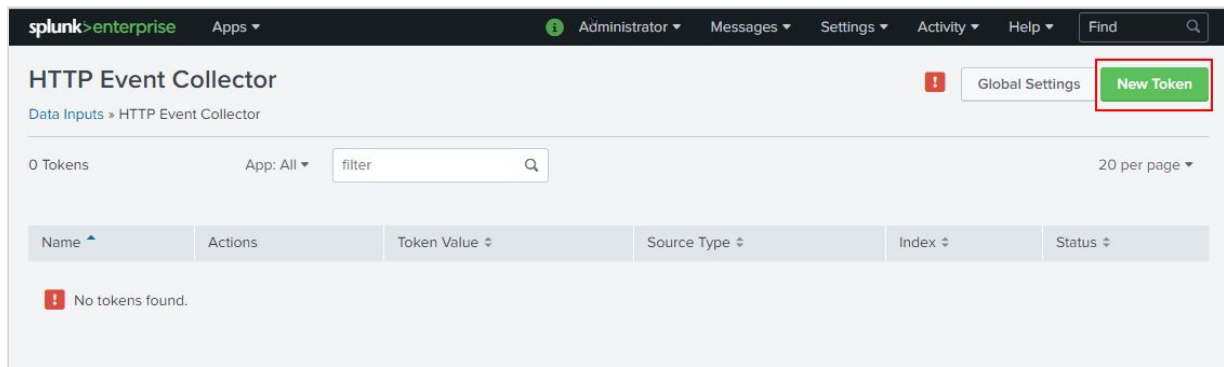


Ensure the panel is configured to look like the example shown above. This should require the following steps:

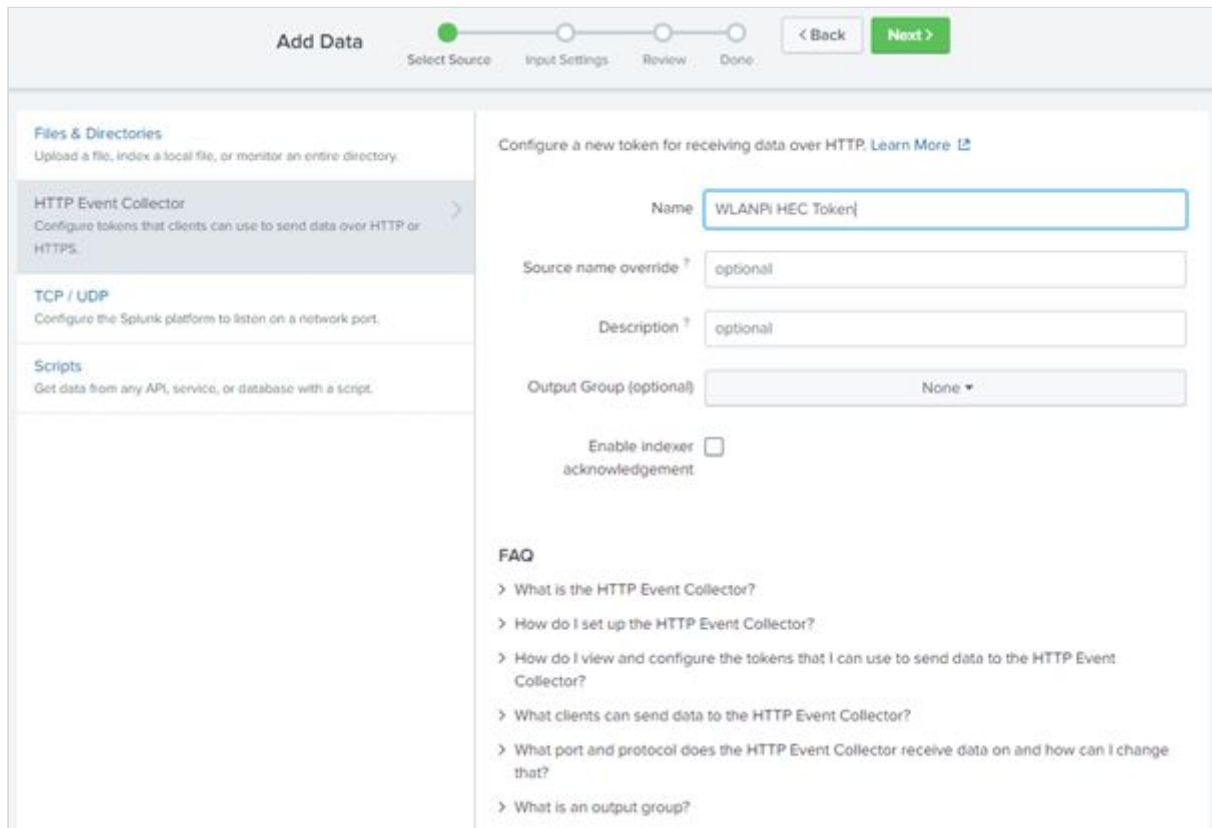
- **Make sure you hit the All Tokens > Enable button** (disabled by default which stops everything working)
- Default Source Type: Structured > _json
- Hit: **Save** to take you back to the HTTP Event Collector page

5.1.3 Create a HEC Token

After returning to the HTTP Event Collector page, hit the **New Token** button. This will start a token creation wizard.



Enter a name for the token (WLANPi HEC Token) then hit **Next >** :



In the next wizard panel select Source type: Select > Structured > _json :

Add Data

Select Source Input Settings Review Done

[< Back](#) [Review >](#)

Input Settings

Optionally set additional input parameters for this data input as follows:

Source type

The source type is one of the default fields that the Splunk platform assigns to all incoming data. It tells the Splunk platform what kind of data you've got, so that the Splunk platform can format the data intelligently during indexing. And it's a way to categorize your data, so that you can search it easily.

Automatic **Select** New

_json

App context

Application contexts are folders within a Splunk platform instance that contain configurations for a specific use case or domain of data. App contexts improve manageability of input and source type definitions. The Splunk platform loads all app contexts based on precedence rules. [Learn More](#)

App Context Apps Browser (appsbrowser)

Scroll down to the indexes and make the following selections:

- Select Allowed Indexes > add all
- Default Index : main

Next, hit the [Review >](#) button:

Add Data

Select Source Input Settings **Review** Done

[< Back](#) [Review >](#)

what kind of data you've got, so that the Splunk platform can format the data intelligently during indexing. And it's a way to categorize your data, so that you can search it easily.

_json

App context

Application contexts are folders within a Splunk platform instance that contain configurations for a specific use case or domain of data. App contexts improve manageability of input and source type definitions. The Splunk platform loads all app contexts based on precedence rules. [Learn More](#)

App Context Search & Reporting (search)

Index

The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. [Learn More](#)

Select Allowed Indexes **Add all** Selected item(s) remove all

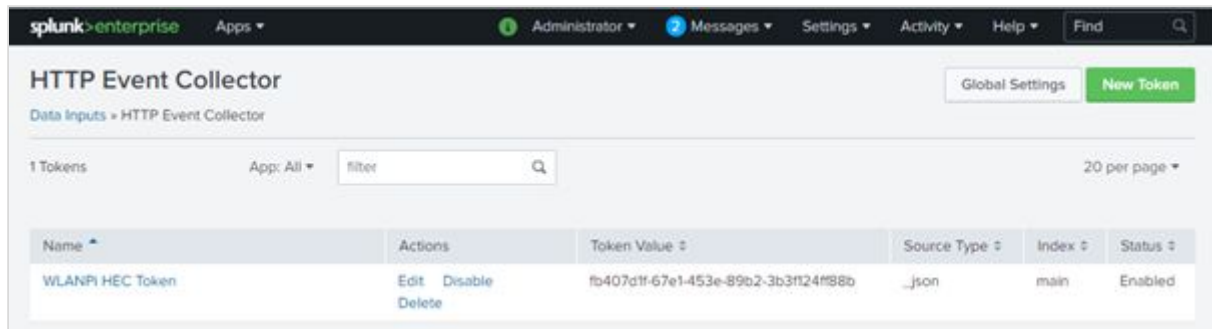
history
main
summary

history
main
summary

Select indexes that clients will be able to select from.

Default Index **main** Create a new index

If you return to Settings > Data Input > HTTPS Event Collector, you will now see the token your WLANPi will need to communicate with the Splunk server:



At this point, the Splunk server is ready to receive data from the WLANPi. Ensure that your WANPi is in Wiperf mode and has been configured with the correct server IP address, port number and the token we have just created above (copy and paste the “Token Value” in to your WLANPi config.ini file).

5.1.4 Perform a Test Search

After a few minutes, when the WLANPi has run a test cycle, data should start to appear in Splunk. The quickest way to check is to do a general search for data in Splunk and see what is being received. Go to “Apps : Search & Reporting > Search & Reporting” (top menu bar) and enter a “*” in the “New Search” text box. Results data should be seen as shown below:

The screenshot shows the Splunk Search & Reporting interface. The search bar contains a wildcard search (*). The results show 4,587 events for the time range 20/12/2019 07:00:00.000 to 21/12/2019 07:46:30.000. The interface includes a timeline visualization and a list of events.

Time	Event
21/12/2019 07:45:48.525	{ [-] renewal_time_ms: 497 time: 1576914348 } Show as raw text source = wiperf-dhcp-splunk sourcetype = _json
21/12/2019 07:45:46.899	{ [-] dns_index: 3 dns_target: google.com lookup_time_ms: 16 time: 1576914346

If your search result looks like this (no results found message), then you need to wait a little longer for data to arrive, or there is likely a comms problem between your WLANPi and Splunk:

The screenshot shows the Splunk Search & Reporting interface with the search bar containing a wildcard search (*). The results show 0 events for the time range 15/12/2019 19:00:00.000 to 16/12/2019 19:57:30.000. The interface displays a message: "No results found. Try expanding the time range."

5.2 Create a Dashboard

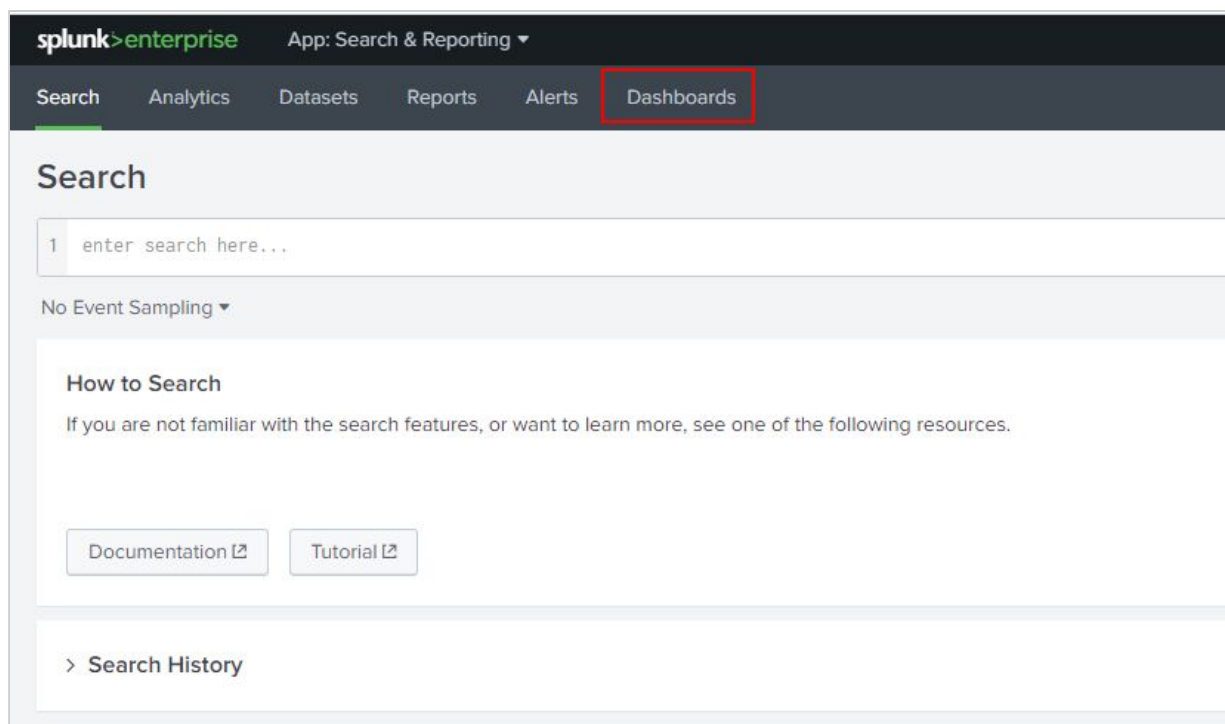
Now that we have data arriving at our Splunk server, we need to view the data in an interesting format. Splunk allows us to create a number of dashboards to visualize our data. We will now create a simple dashboard to demonstrate the visualization capabilities.

In the WLANPi's `/home/wlanp/wiperf/dashboards` directory, a number of pre-canned dashboard files have been provided to allow a dashboard to be copied and pasted easily. These are also available on the GitHub page of the Wiperf project:

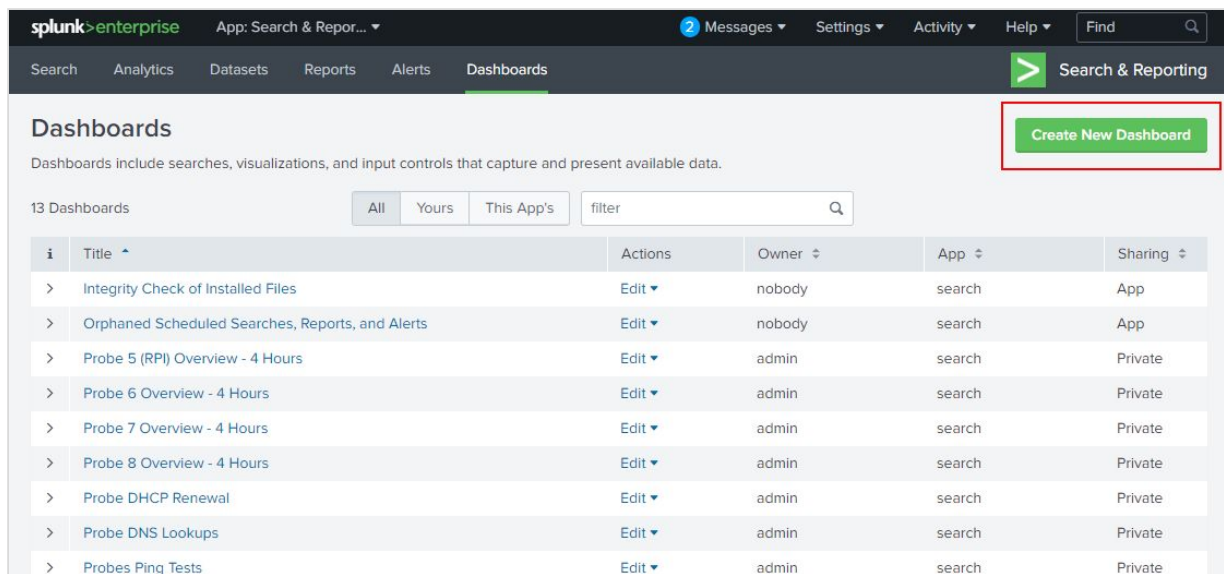
- <https://github.com/wifinigel/wiperf/tree/master/dashboards>

Use an SFTP client to pull the “probe_summary.xml” file from your WLANPi or open the file on the GitHub page and select “Raw” to copy and paste the code in to a local file on your laptop.

In the Splunk GUI, go to “Apps : Search & Reporting > Search & Reporting” (top menu bar) and hit the “Dashboards” link:



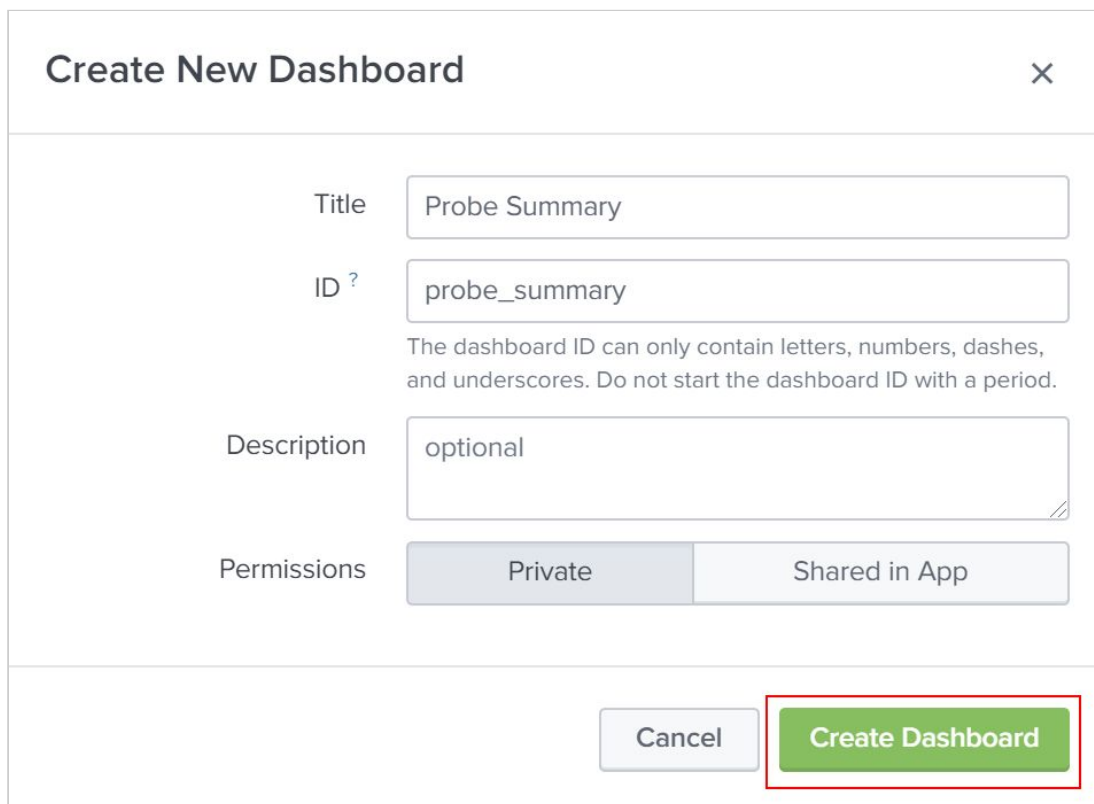
Hit the **Create New Dashboard** button:



The screenshot shows the Splunk interface with the 'Dashboards' tab selected. A green button labeled 'Create New Dashboard' is highlighted with a red box in the top right corner. Below the header, there is a table listing 13 dashboards. The table has columns for Title, Actions, Owner, App, and Sharing.

i	Title	Actions	Owner	App	Sharing
>	Integrity Check of Installed Files	Edit	nobody	search	App
>	Orphaned Scheduled Searches, Reports, and Alerts	Edit	nobody	search	App
>	Probe 5 (RPI) Overview - 4 Hours	Edit	admin	search	Private
>	Probe 6 Overview - 4 Hours	Edit	admin	search	Private
>	Probe 7 Overview - 4 Hours	Edit	admin	search	Private
>	Probe 8 Overview - 4 Hours	Edit	admin	search	Private
>	Probe DHCP Renewal	Edit	admin	search	Private
>	Probe DNS Lookups	Edit	admin	search	Private
>	Probes Ping Tests	Edit	admin	search	Private

In the pop-up panel, enter a dashboard name and hit the **Create Dashboard** button:

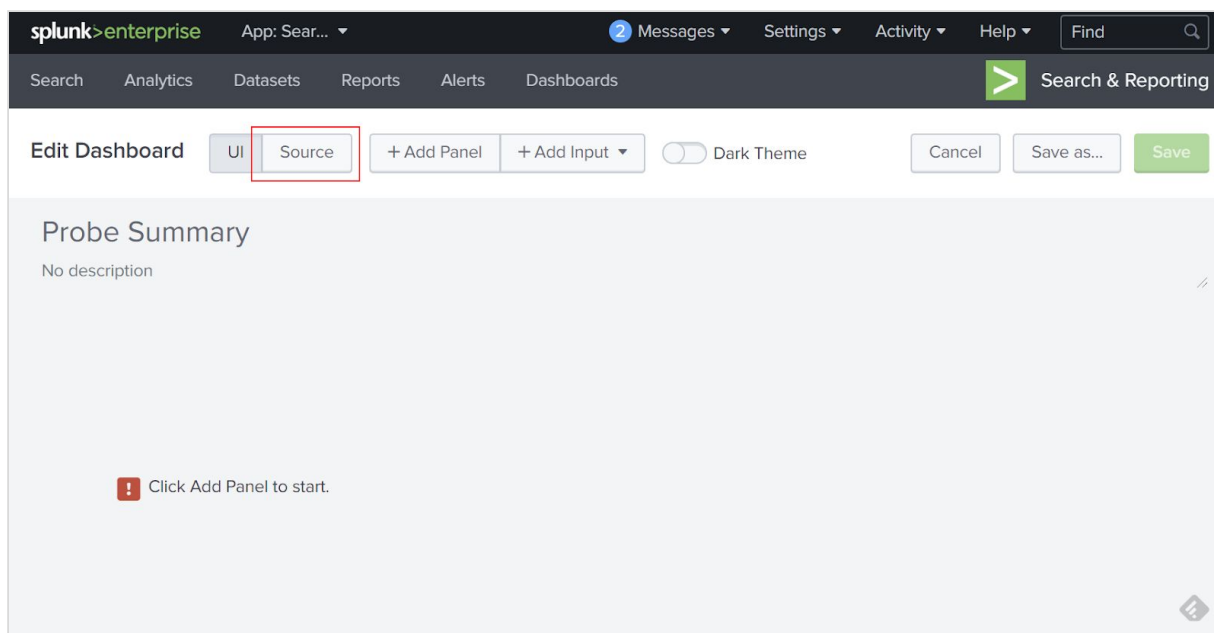


The screenshot shows the 'Create New Dashboard' pop-up panel. It contains the following fields and options:

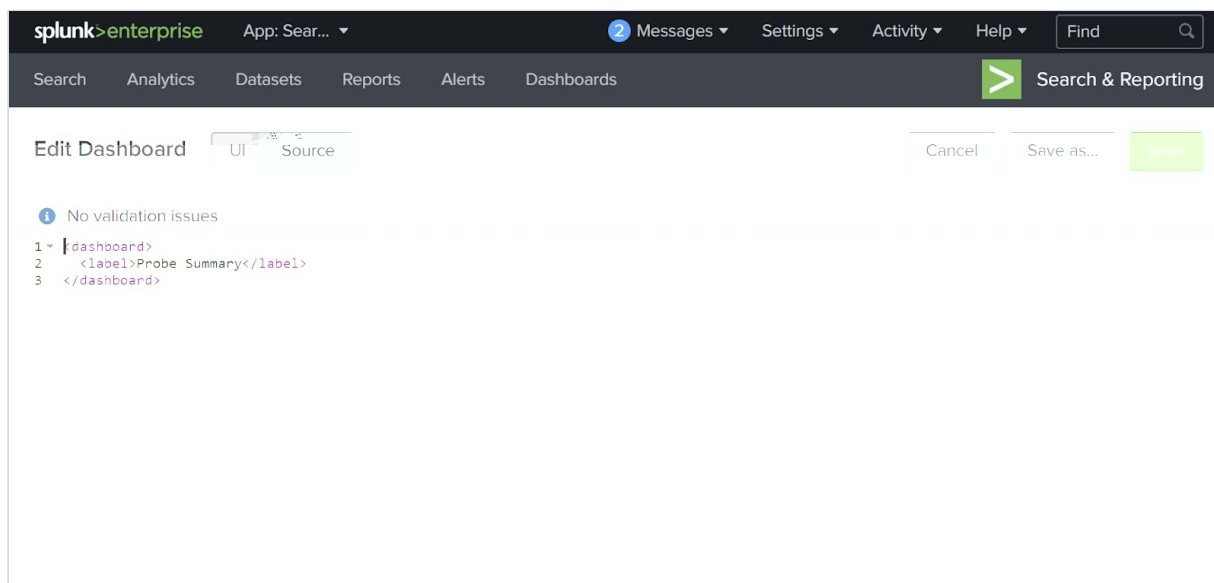
- Title:** Probe Summary
- ID:** probe_summary
- Description:** optional
- Permissions:** Private (selected) and Shared in App

At the bottom, there are two buttons: 'Cancel' and 'Create Dashboard'. The 'Create Dashboard' button is highlighted with a red box.

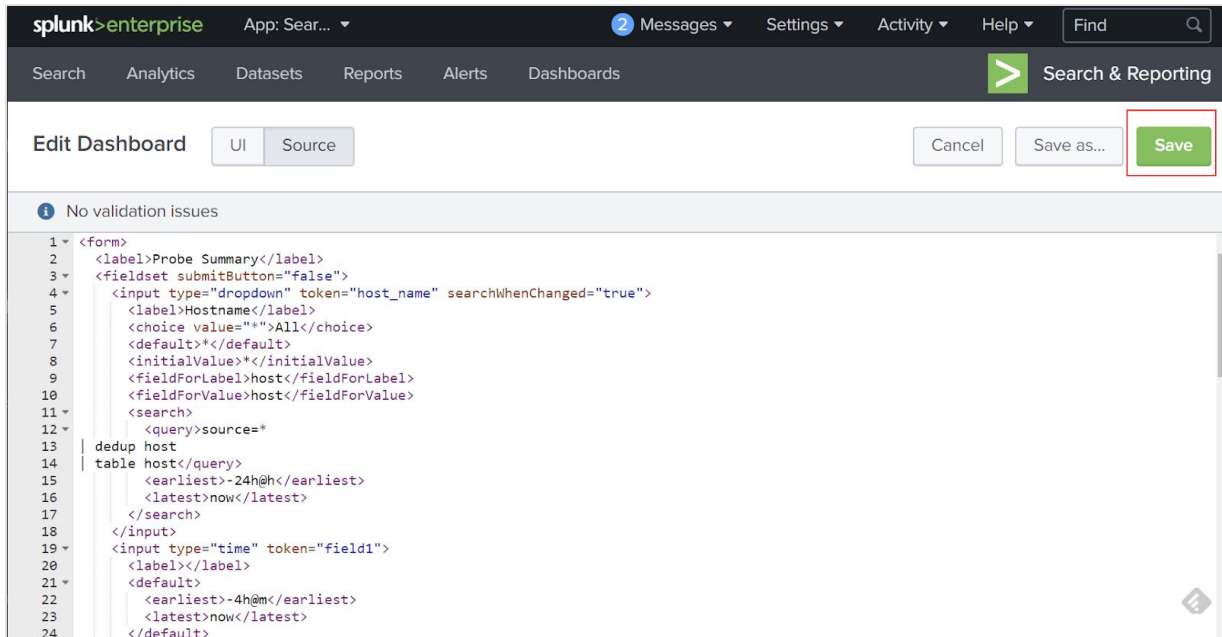
In the “Edit Dashboard” panel that opens, hit the “Source” button:



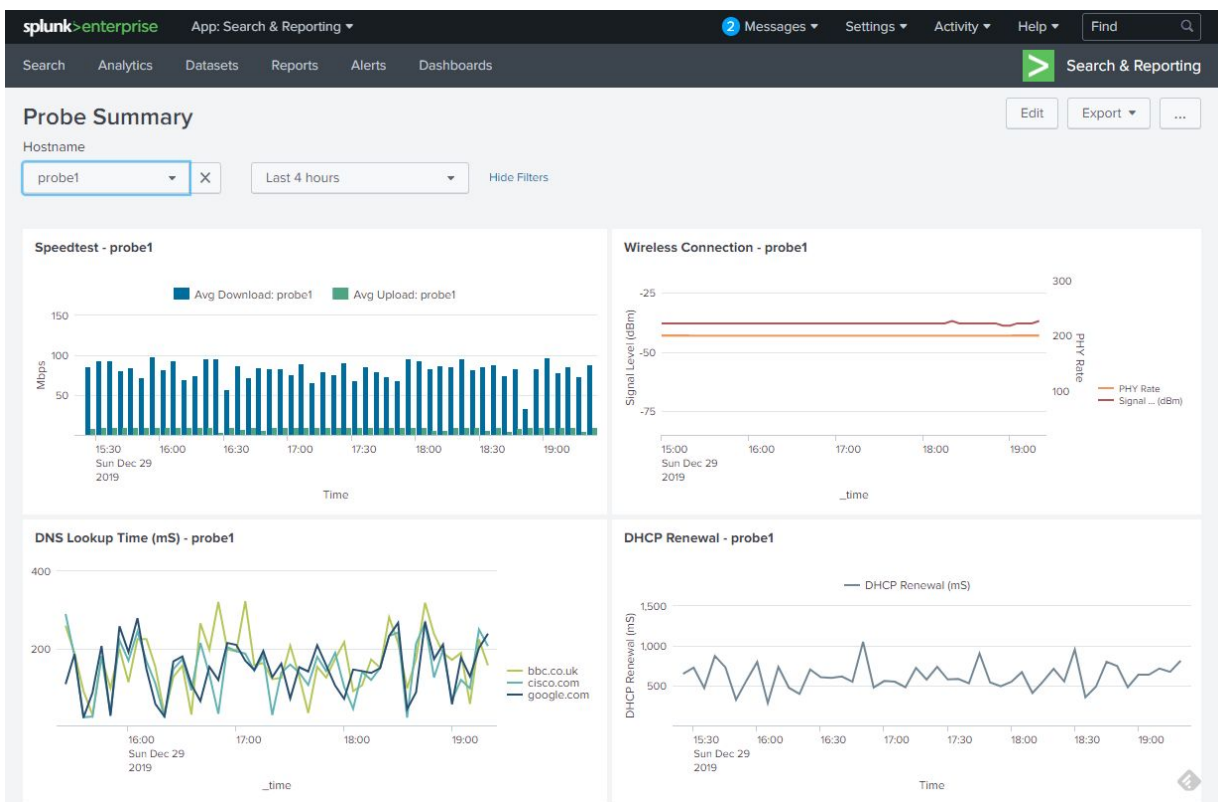
By default, some basic XML configuration will exist in the dashboard definition:



Open up the dashboard definition file previously downloaded from your WLANPi or the GitHub site in a text editor. Then simply paste in the code as shown below (make sure the original code was all removed):



After hitting the **Save** button, the dashboard will now be shown:



Using the hostname and time period selector above the graphs, different probes and reporting periods may be viewed.