carahsoft.

splunk>

General Splunk Configuration

This session will cover configuring your Splunk instance, as well as setting up forwarders and applications.

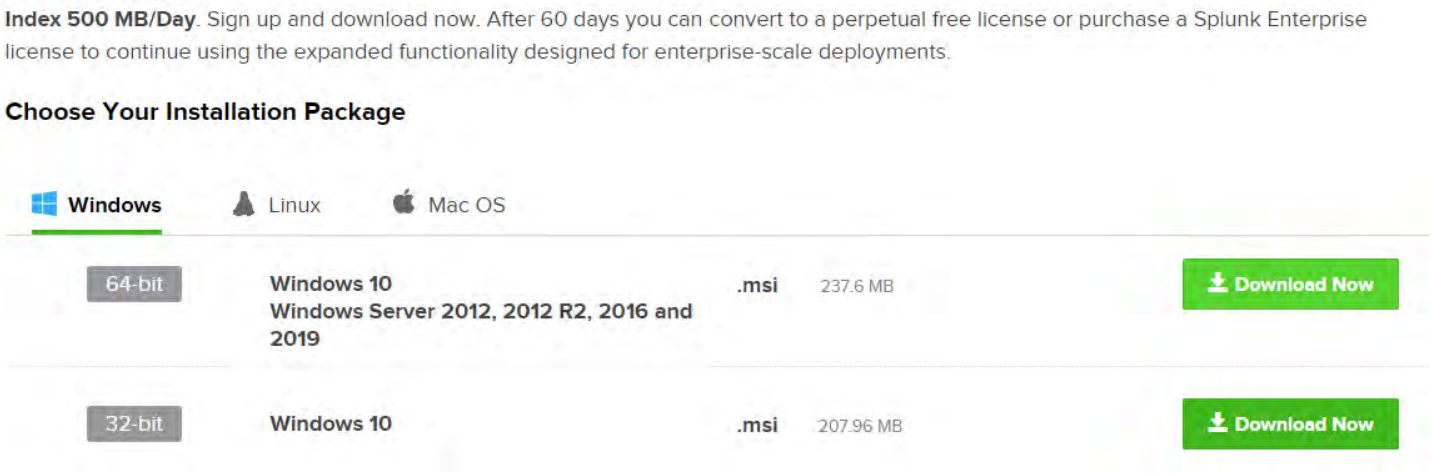
Prerequisites:

- Windows operating system (recommended Windows 10, older may work but please test first)
- Full administrative access to system you are using (including ability to run command prompt as admin)
- Notepad++
- 7zip or winzip
- The following ports available; 8000, 8001, 8080, 9997

Part One: Install & Customize Splunk

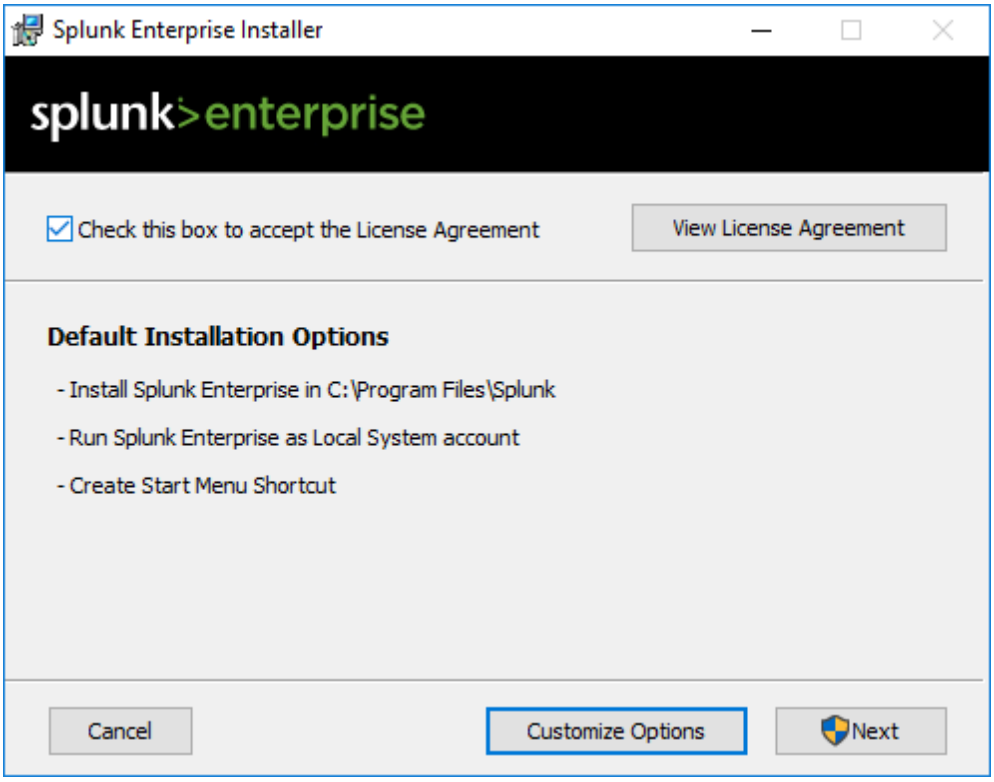
If Splunk is already installed on your computer, proceed to the next step.

If Splunk is not installed, go to https://splunk.com/en_us/download/splunk-enterprise.html and download the appropriate msi. Note that you will need to log into your Splunk account in order to download the package.

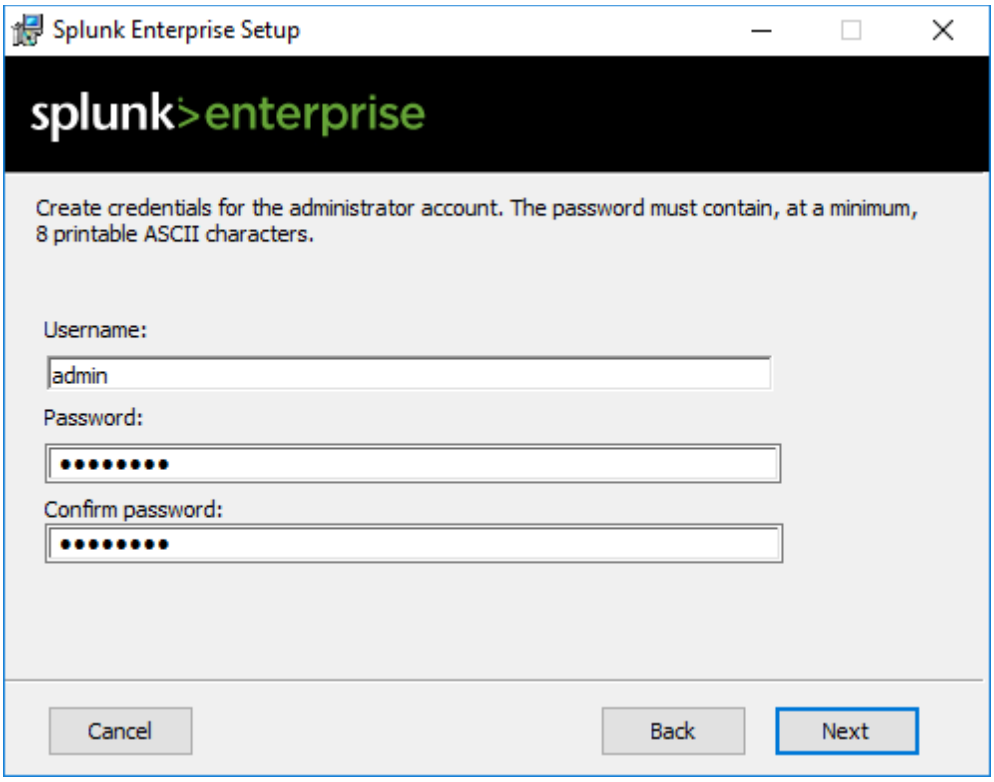


Once downloaded, click to run the msi.

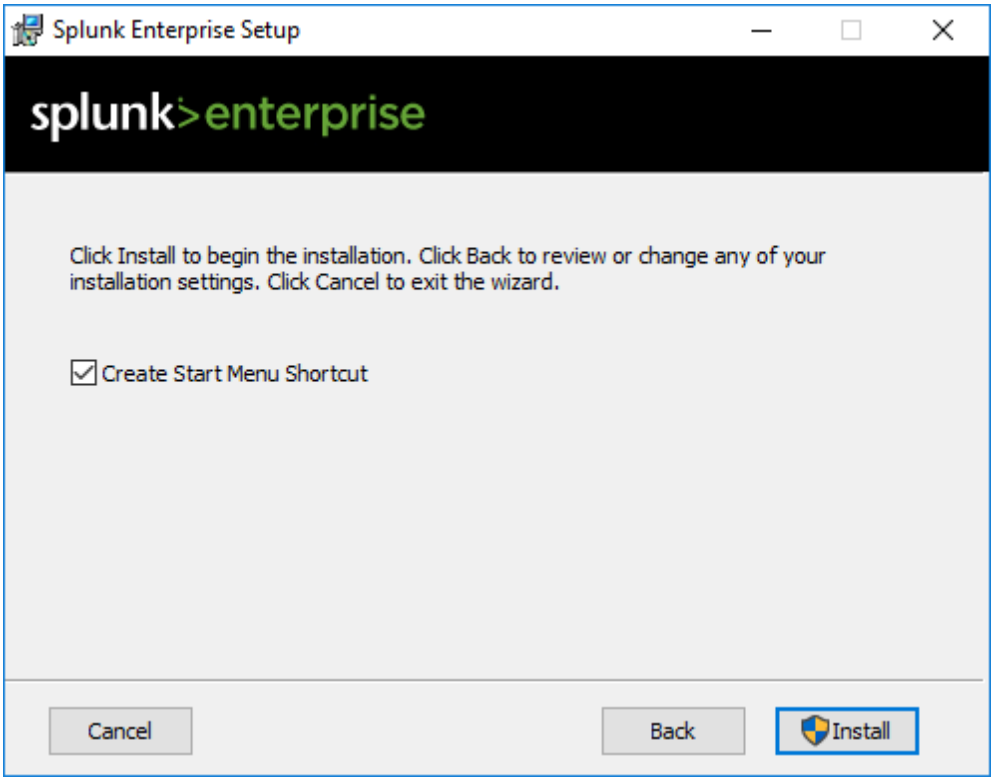
- Note that you can choose the customize options button to install Splunk into a different directory.



Click '**Next**' and create your **username- 'admin'** and **password 'admin123'**



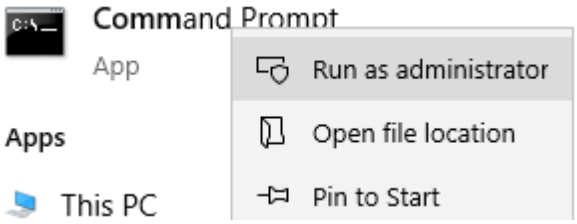
Click '**Next**' and then '**Install**'



The wizard should now install Splunk.

You're now the proud owner of a Splunk instance. Unfortunately, given the login we created, you're also the owner of a relatively unsecure instance. Let's customize our login info and keep some easy password-guessing from compromising our new tool.

Open your command prompt and right click '**run as administrator**'



Navigate to your bin directory within Splunk- from here we can issue commands to our Splunk instance.

```
C:\Program Files>cd C:\Program Files\Splunk\bin

C:\Program Files\Splunk\bin>
```

By using the format '**splunk edit user admin -password newpassword -auth admin:oldpassword'** we can make changes here. Let's set it to **C@r@hSoft56**!

```
C:\Program Files\Splunk\bin>splunk edit user admin -password C@r@hSoft56! -auth
admin:admin123
User admin edited.

C:\Program Files\Splunk\bin>
```

Now we need to create a user role for our coworkers who will be using Splunk. But we don't want to give them full administrative permissions, so we'll add them as a user. Note that we can specify any of the available roles defined in Splunk. We could also do this through the GUI later if we wanted.

This will take the format '**splunk add user Dallon -password changeme -role user -auth admin: C@r@hSoft56!**' (or any password you will remember)

```
C:\Program Files\Splunk\bin>splunk add user Dallon -password changeme -role user
 -auth admin:C@r@hSoft56!
User added.

C:\Program Files\Splunk\bin>
```

We're almost done getting everything up and running. By default, Splunk web will use the port 8000. I already have another tool utilizing that port, so we'll need to change it- 8001 will work fine. We can also use this in cases where a firewall is blocking specific ports or a directing agency has given us a set of ports to use for given tools. For this type: **'splunk set web-port 8001'**

```
C:\Program Files\Splunk\bin>splunk set web-port 8001
The server's web port has been changed.
You need to restart the Splunk Web Server (splunkweb) for your changes to take effect.
```

Now all we need to do is command Splunk to restart ('**splunk restart**') and we're ready to go. Note that during the restart we can see all the ports and processes being used and identify any issue (or any additional ports we need to change).

```
Checking prerequisites...
        Checking http port [8001]: open
        Checking mgmt port [8089]: open
        Checking appserver port [127.0.0.1:8065]: open
        Checking kvstore port [8191]: open
        Checking configuration... Done.
        Checking critical directories...        Done
        Checking indexes...
                (skipping validation of index paths because not running as LocalSystem)
                Validated: _audit _internal _introspection _telemetry _thefishbucket history main summary
        Done
        Checking filesystem compatibility...  Done
        Checking conf files for problems...
        Done
        Checking default conf files for edits...
        Validating installed files against hashes from 'C:\Program Files\Splunk\splunk-7.3.1-bd63e13aa157-windows
-64-manifest'
        All installed files intact.
        Done
```

Once Splunk has restarted, open up Splunk Enterprise and confirm that you can login as admin through the GUI.

Part Two: Forwarder and Applications

Now that we have Splunk up and running and have seen how easy it is to build dashboards, let's bring in some of our own data.

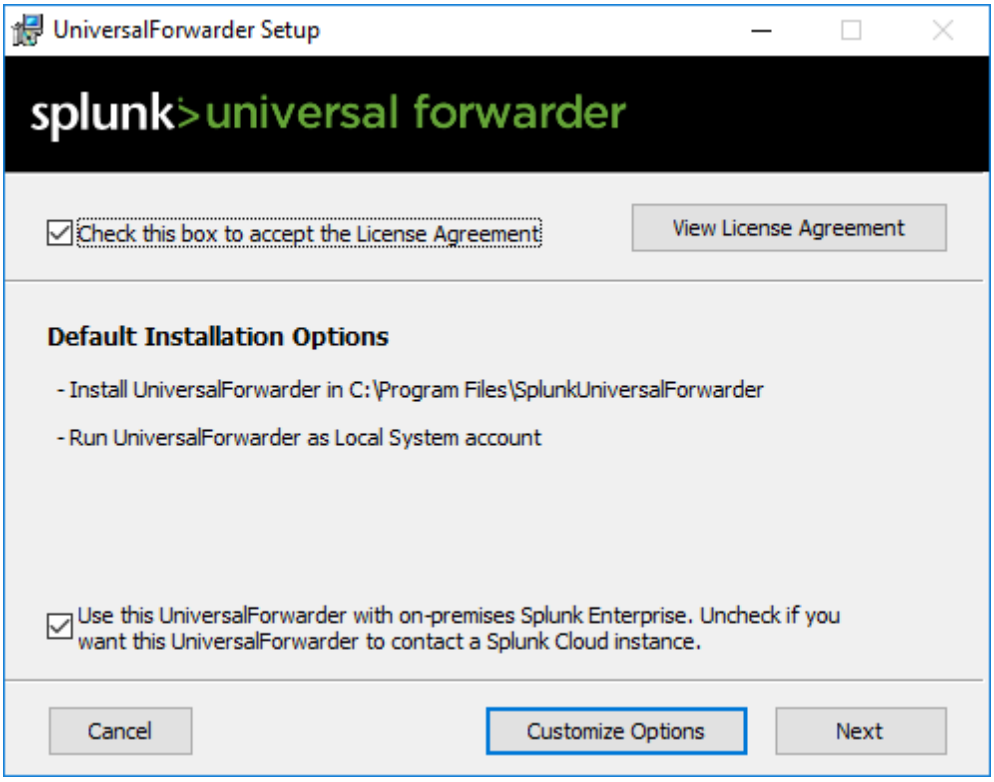
Today we'll be installing forwarders on the same machine that is hosting Splunk- for the ease of training resources our forwarder and indexer/search head are on the same machine, but we will be treating these as two separate entities and they will function exactly the same as if our forwarder was installed on a separate server.

The first thing we need to do is download a forwarder onto our host from Splunk's website.

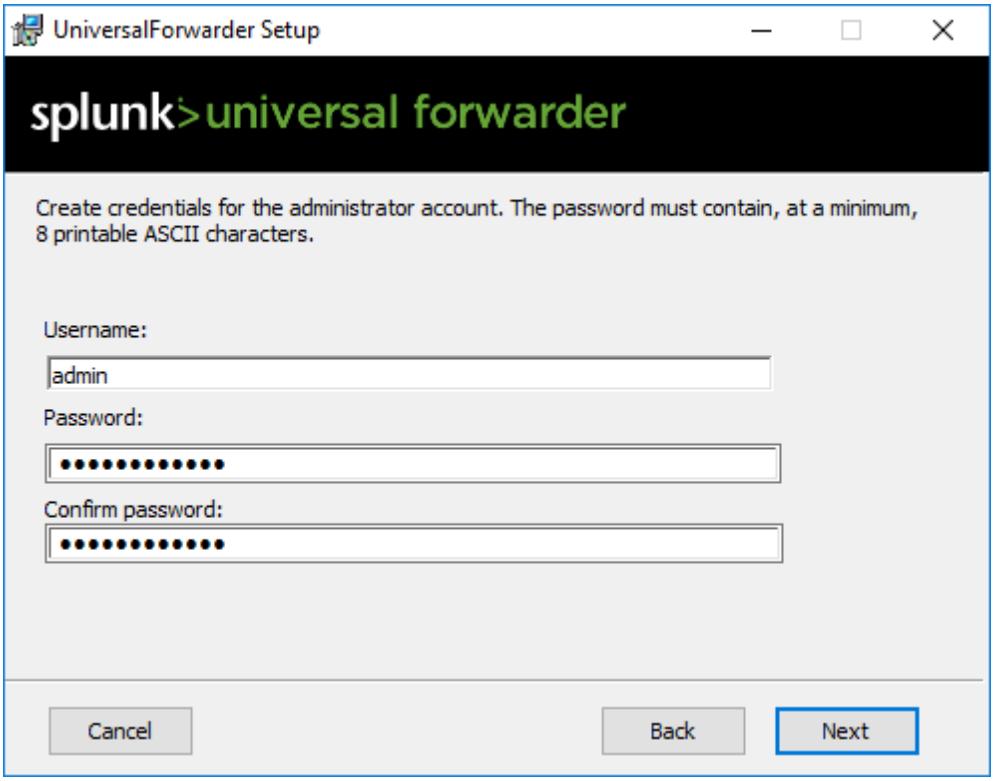
Also, make sure you have both notebook ++ and 7-zip downloaded.

https://www.splunk.com/en_us/download/universal-forwarder.html

Click the msi to run it. Note that at this stage if we were using Splunk Cloud we need to specify that by unchecking the box here.

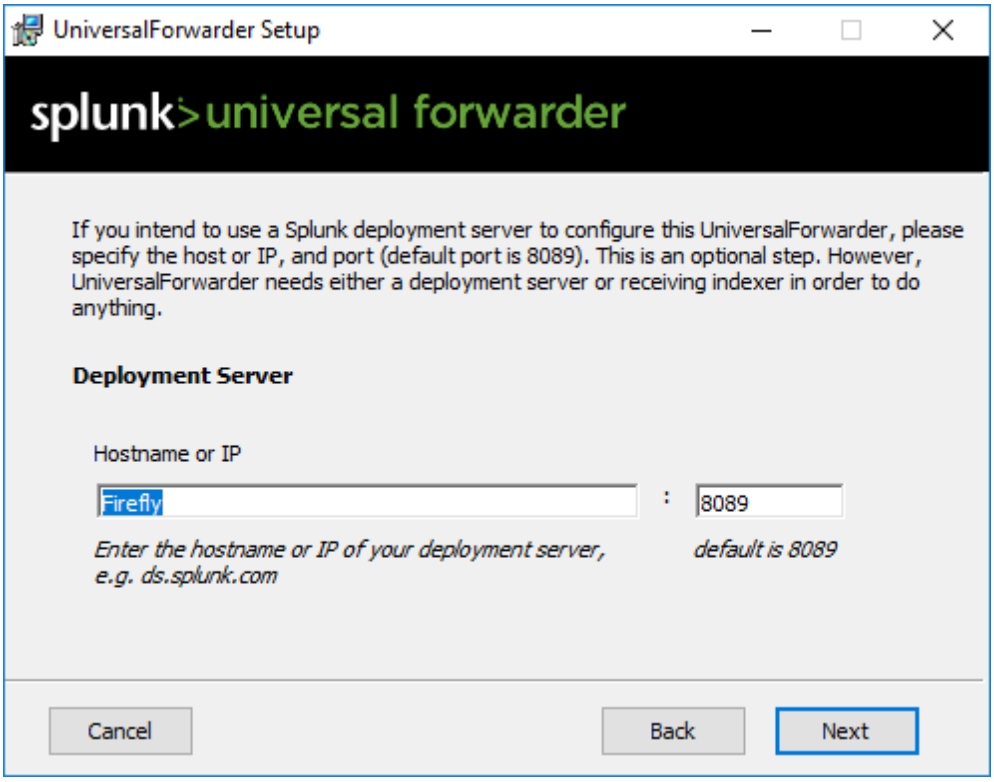


Note that on the next step, when the UF asks us to specify credentials that these are not automatically the same as our Splunk instance. For the sake of time and complexity, we'll today use the same username/password that we changed our main Splunk instance to in part 1.

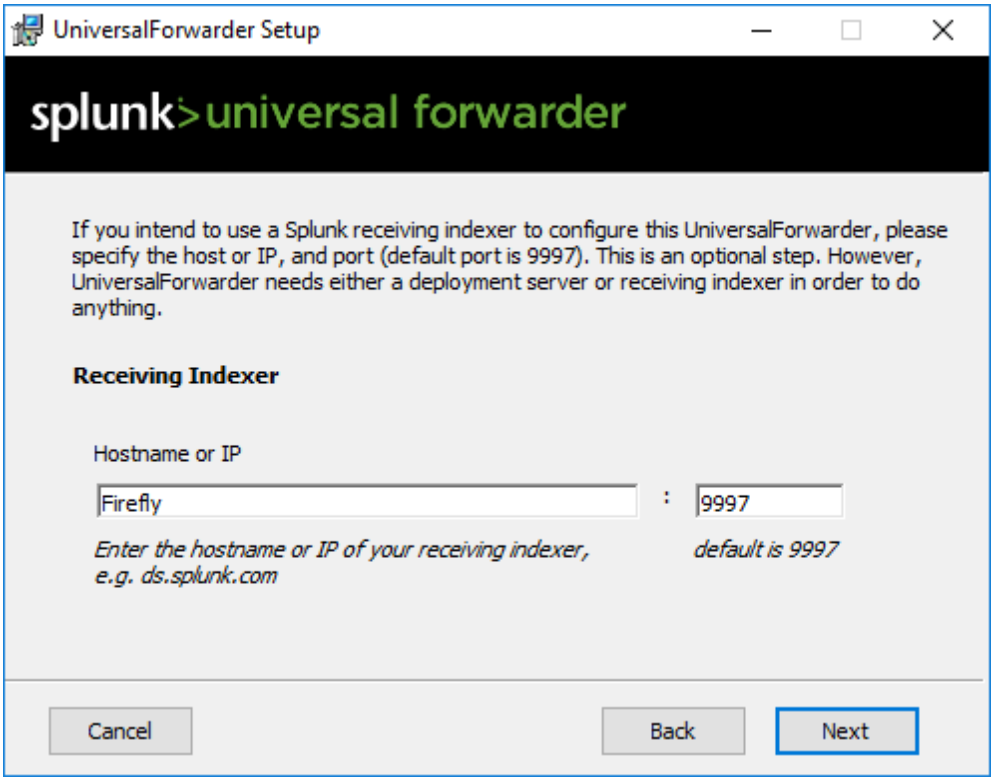


Splunk will next ask us if we would like to assign this forwarder to a deployment server. A Deployment Server is a Splunk Enterprise instance that acts as a centralized configuration manager, grouping together and collectively managing any number of Splunk Enterprise instances. While it takes some additional set up and maintenance in the beginning, this is often the fastest and most effective way to manage your Splunk environment. Alternatively, you could use tools like Chef or Puppet to accomplish the same task- but a deployment server is native to your Splunk environment and comes at no additional cost to you.

Note that we can specify the IP address or the hostname here. Either will work, but it's worth thinking about what will happen if you lose connectivity to your DNS server and have specified the hostname over the IP address.



We'll next specify our receiving indexer. In smaller environments, this is most likely our deployment server as well- as our Splunk deployment grows and we add more indexers, this may or may not be the case.



Click install and then finish.

Now open up command prompt and right click 'run as administrator'

Go to C:\Program Files\SplunkUniversalForwarder\bin – from here we can issue commands to our forwarder. Let's check and see if our forwarder is connected to our indexer'

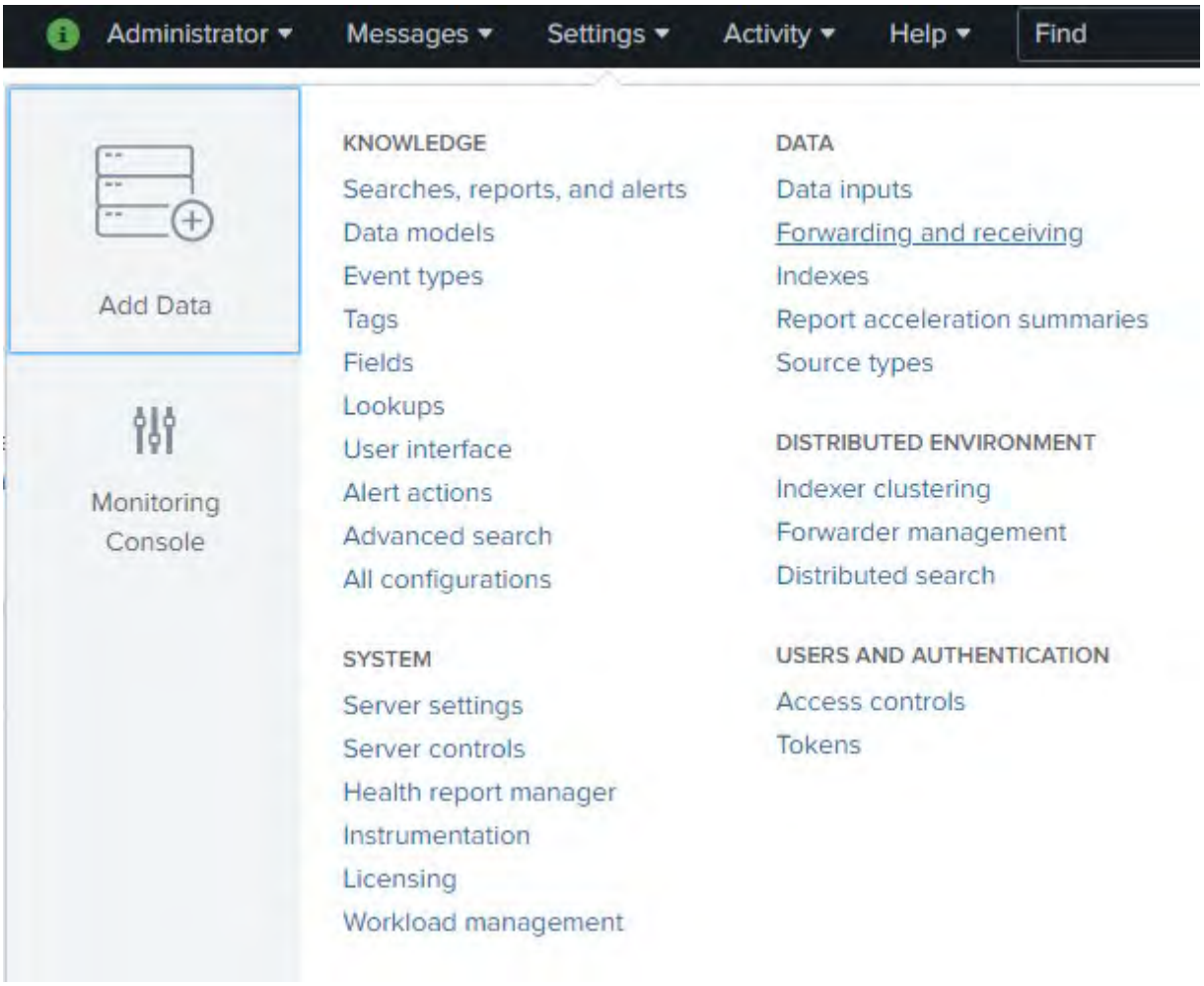
Enter the command 'splunk list forward-server' (you'll be prompted to login with the credentials you created during the install phase)

Note that at this point you should have a 'configured but inactive forward'

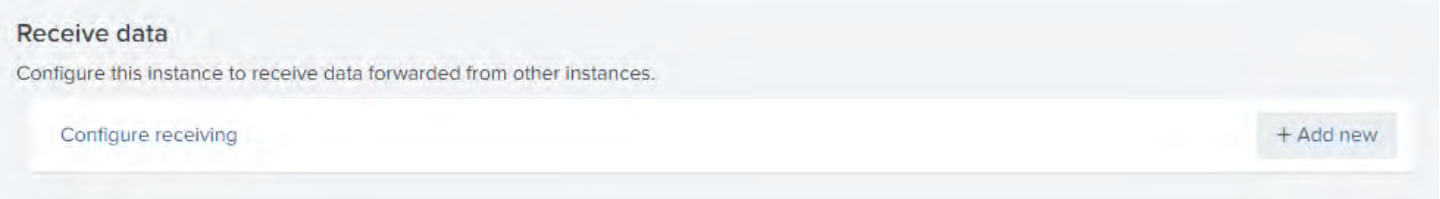
```
C:\Program Files\SplunkUniversalForwarder\bin>splunk list forward-server
Your session is invalid.  Please login.
Splunk username: admin
Password:
Active forwards:
        None
Configured but inactive forwards:
        Firefly:9997
```

This is because while our forwarder is sending, our indexer is not yet receiving.

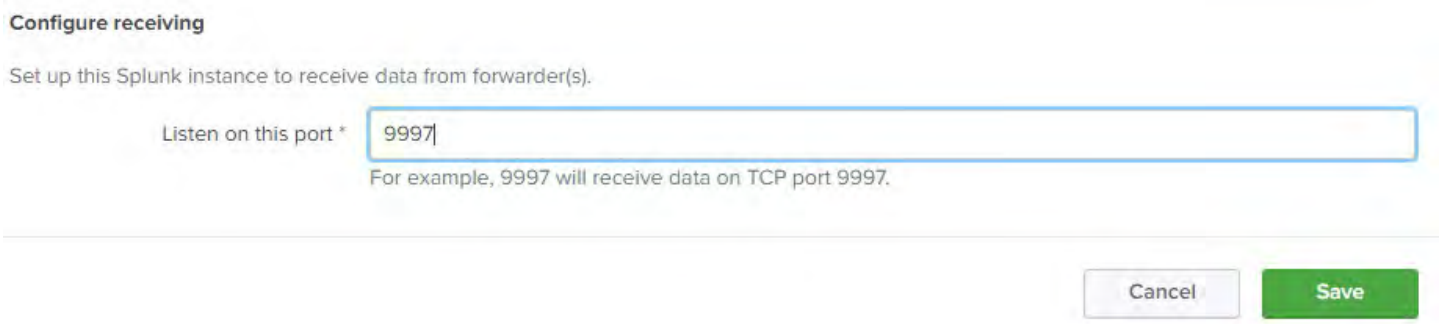
Let's log into our main Splunk instance through the GUI. Go to settings>forwarding and receiving



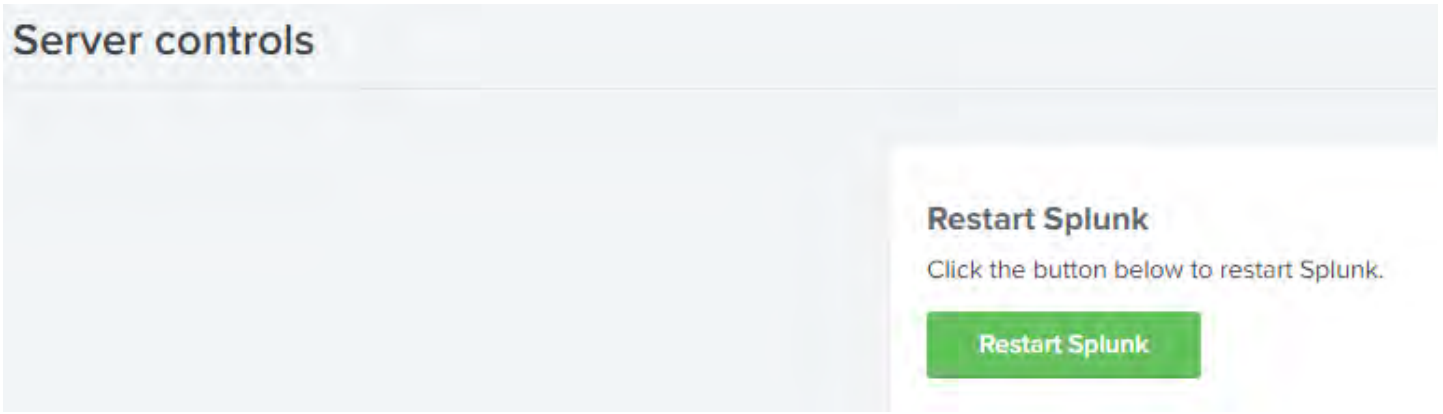
Once there, click 'add new' in receiving



Configure Splunk to listen on the port we forwarded to by entering 9997 and clicking save



Now restart Splunk. This can be done via the CLI like in part 1, or you can go to settings>server controls>restart Splunk

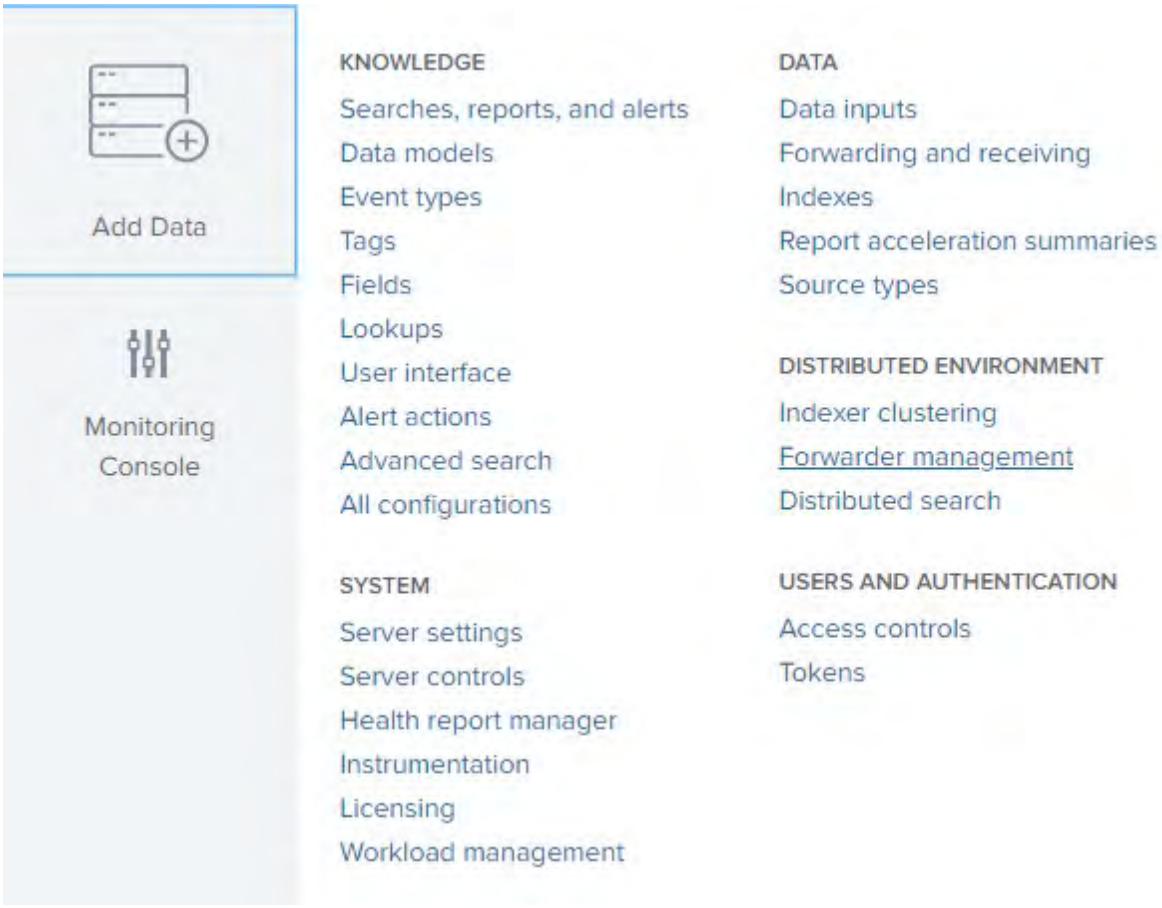


Let's check in at our forwarder again and see if the connection is now active. Run the command 'splunk list forward-server' again and you should see the below

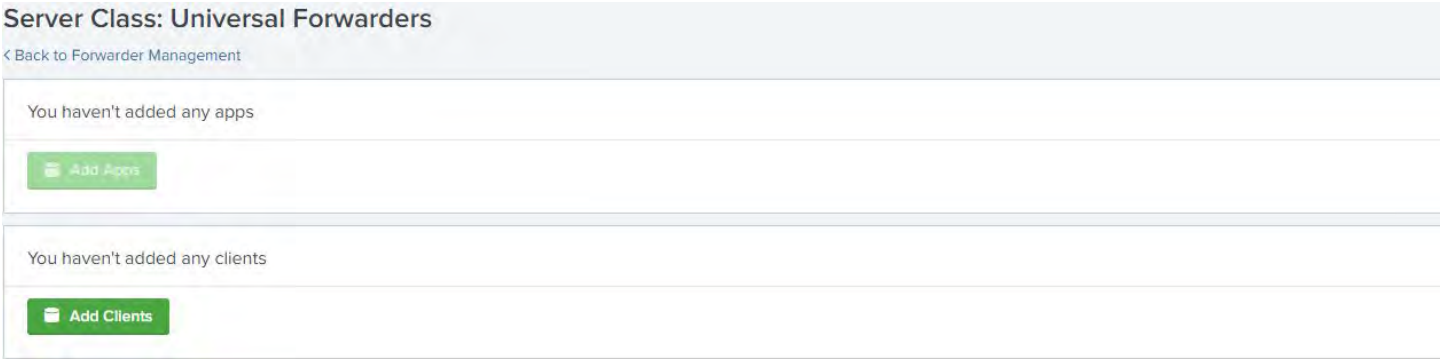
```
C:\Program Files\Splunk\bin>cd C:\Program Files\SplunkUniversalForwarder\bin

C:\Program Files\SplunkUniversalForwarder\bin>splunk list forward-server
Active forwards:
        Firefly:9997
Configured but inactive forwards:
        None
```

Now we know our connection is working. Let's go back to our Splunk GUI and go to Settings>Distributed Environment>Forwarder management. There we should be able to see our deployment client listed.

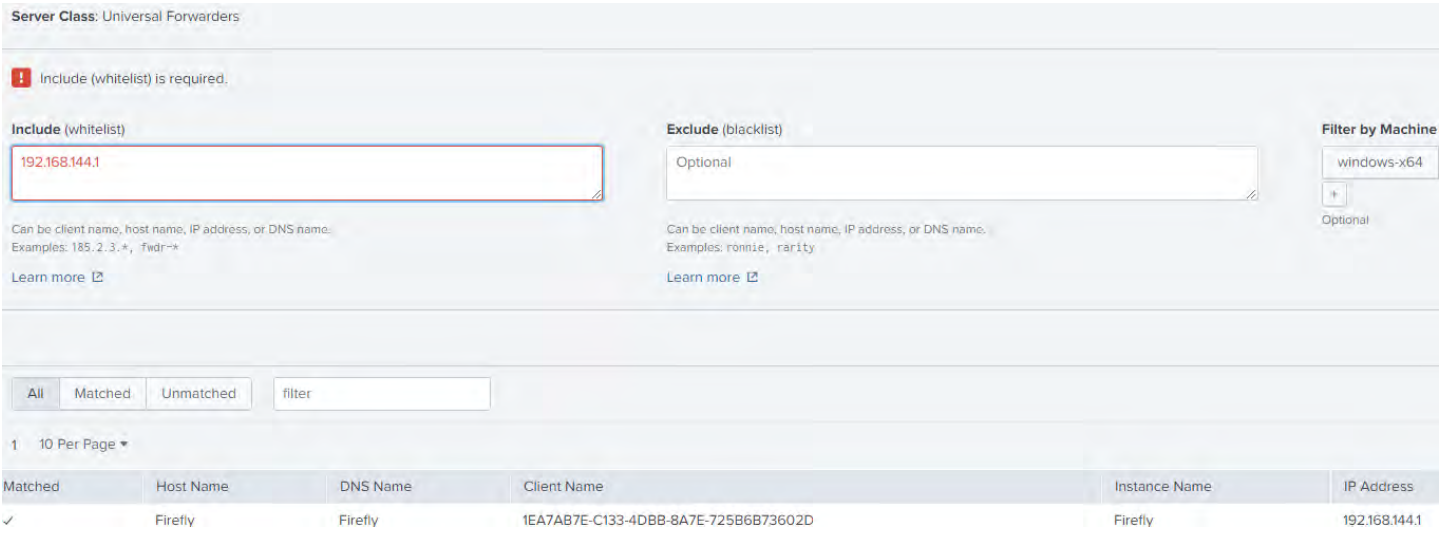


Click ‘Server Classes’ just to the left of ‘Clients’ and hit the green ‘New Server Class’ button. We’ll name this one ‘Universal Forwarders’. Then select ‘Add Clients’



Note that we can whitelist by hostname, IP address, or other criteria. We can also exclude specific clients as our environment grows and we have more clients.

Let's whitelist our clients IP and save



Now we have our forwarder installed and configured, we've assigned it to a server class that will easily let us manage it and other similar forwarders as our deployment grows, and we know that we're able to receive data on our indexer. However, we aren't collecting any data yet. We need to tell this forwarder what we want to collect from the client. We can now download add-ons to determine what we want to bring in to Splunk and applications to utilize prebuilt and out of the box dashboards on Splunkbase.

END OF SESSION

Conclusion

So just to recap, we went over how to install Splunk, set up universal forwarders, and how to configure users and set permissions.

We first went into the CLI to make sure our Splunk Instance password is secure. We then went into changing what port Splunk is running on in the CLI.

Installing and setting universal forwarders was the next steps and we went into deployment servers and receiving indexers along with configuring everything within the Splunk GUI.

Once we had our universal forwarder set up and running properly, we can download any applications and add-ons from Splunk base to start utilizing our forwarders and real time data from our own environment.