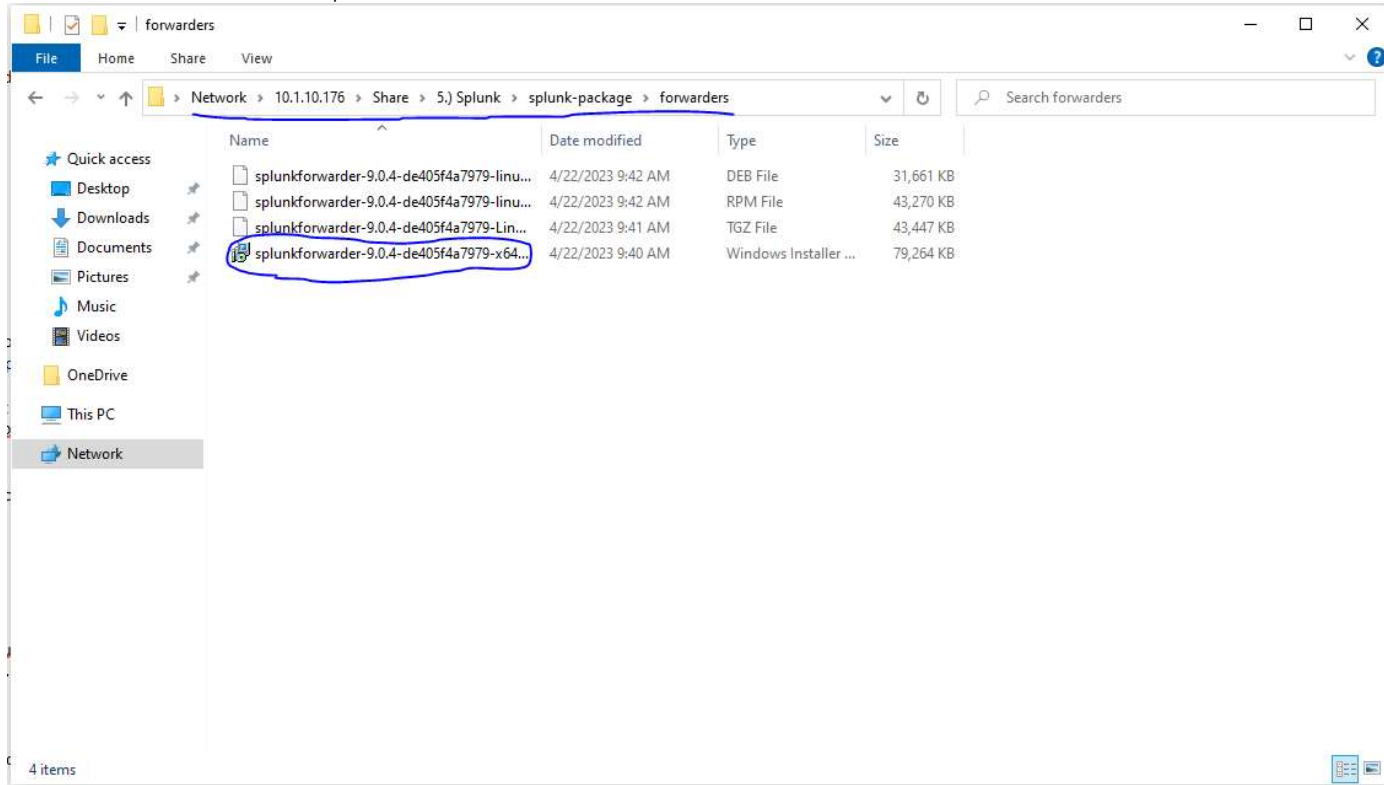


Splunk Forwarder (WINDOWS)

Thursday, March 28, 2024 12:18 PM

On the windows machine:

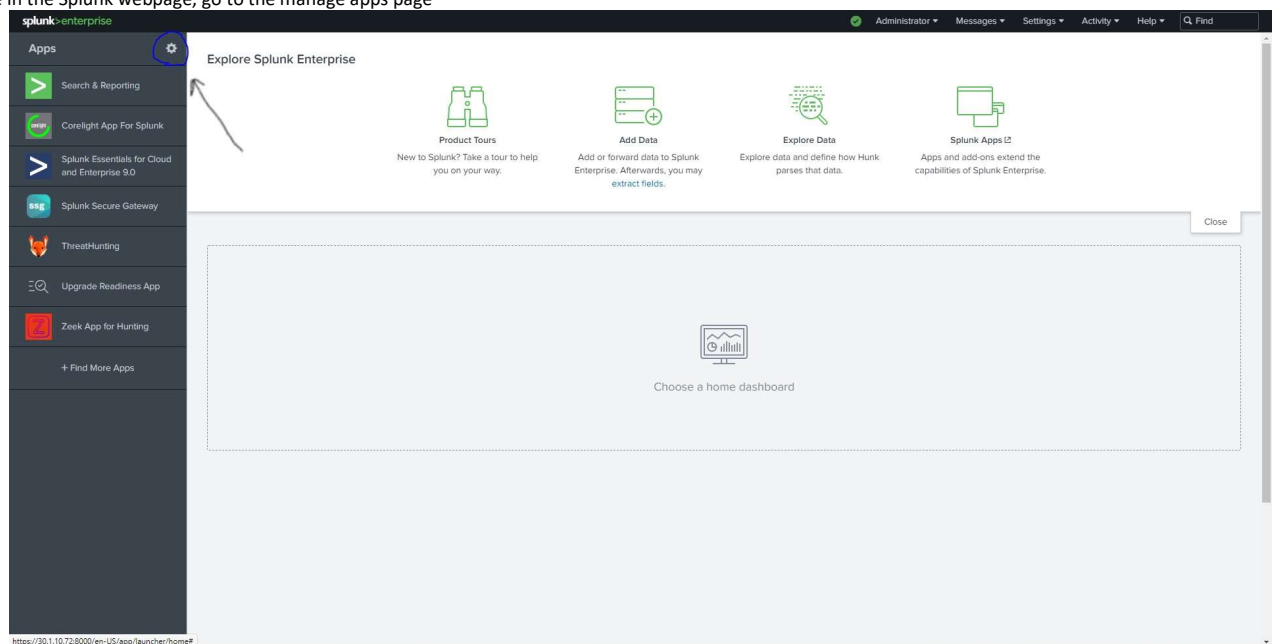
- 1) Install the forwarder onto the host
 - a. Double click the msi and follow the setup wizard



- 1) It will need to script out

- 2) On the Splunk webpage

- a. Create an app
 - i. Once in the Splunk webpage, go to the manage apps page



- ii. Once in the Manage Apps Page, you will click on "Create App"

splunk>enterprise Apps ▾ Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Apps

Showing 1-25 of 32 items

filter

25 per page ▾

◀ Prev 1 2 Next ▶

Name ▴	Folder name ▴	Version ▴	Update checking ▴	Visible ▴	Sharing ▴	Status ▴	Actions
Corelight App For Splunk	CorelightForSplunk	2.4.6	Yes	Yes	Global Permissions	Enabled Disable	Launch app Edit properties View objects View details on Splunkbase
SplunkForwarder	SplunkForwarder		Yes	No	App Permissions	Disabled Enable	
SplunkLightForwarder	SplunkLightForwarder		Yes	No	App Permissions	Disabled Enable	
Splunk Add-on for Sysmon	Splunk_TA_microsoft_sysmon	3.1.0	Yes	No	Global Permissions	Enabled Disable	Edit properties View objects View details on Splunkbase
Splunk Add-on for Zeek	Splunk_TA_zeek	10.5	Yes	No	Global Permissions	Enabled Disable	Edit properties View objects View details on Splunkbase
TA-suricata-4	TA-suricata-4	2.3.4	Yes	No	Global Permissions	Enabled Disable	Edit properties View objects View details on Splunkbase
ThreatHunting	ThreatHunting	1.5.1	Yes	Yes	Global Permissions	Enabled Disable	Launch app Edit properties View objects View details on Splunkbase
Log Event Alert Action	alert_logevent	9.0.4.1	Yes	No	App Permissions	Enabled Disable	Edit properties View objects
Webhook Alert Action	alert_webhook	9.0.4.1	Yes	No	App Permissions	Enabled Disable	Edit properties View objects
Apps Browser	appsbrowser	9.0.4.1	Yes	No	App Permissions	Enabled	Edit properties View objects
DCO Tools	dco_tools	1.0.0	Yes	No	App Permissions	Enabled Disable	Edit properties View objects
Introspection_generator_addon	Introspection_generator_addon	9.0.4.1	Yes	No	App Permissions	Enabled Disable	Edit properties View objects
journald_input	journald_input		Yes	No	App Permissions	Enabled Disable	Edit properties View objects
Home	launcher		Yes	Yes	App Permissions	Enabled	Launch app Edit properties View objects
learned	learned		Yes	No	App Permissions	Enabled Disable	Edit properties View objects
legacy	legacy		Yes	No	App Permissions	Disabled Enable	
Upgrade Readiness App	python_upgrade_readiness_app	4.0.3	Yes	Yes	App Permissions	Enabled Disable	Launch app Edit properties View objects View details on Splunkbase
sample data	sample_app		Yes	No	App Permissions	Disabled Enable	
Search & Reporting	search	9.0.4.1	Yes	Yes	App Permissions	Enabled	Launch app Edit properties View objects
Splunk Dashboard Studio	splunk-dashboard-studio	17.4	Yes	Yes	App Permissions	Enabled Disable	Launch app Edit properties View objects
Splunk Archiver App	splunk_archiver	1.0	Yes	No	App Permissions	Enabled Disable	Edit properties View objects View details on Splunkbase
Splunk Assist	splunk_assist	1.0.3	No	No	App Permissions	Enabled Disable	Edit properties View objects View details on Splunkbase
https://30.110.72.8000/en-us Cloud and Enterprise 9.0	splunk_essentials_9_0	1.0.0	Yes	Yes	App Permissions	Enabled Disable	Launch app Edit properties View objects View details on Splunkbase

iii. Once you click on "Create App", you will see the image below

splunk>enterprise Apps ▾ Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Add new

Apps ▸ Add new

Name

Give your app a friendly name for display in Splunk Web.

Folder name *

This name maps to the app's directory in \$SPLUNK_HOME/etc/apps/.

Version

App version.

Visible ☐ No ☒ Yes

Only apps with views should be made visible.

Author

Name of the app's owner.

Description

Enter a description for your app.

Template **barebones**

These templates contain example views and searches.

Upload asset No file chosen

Can be any html, js, or other file to add to your app.

1) The following is what you will fill in, unless told otherwise

- Name = DCO Tools
- Foldername = dco_tools
- Version = 1.0.0
- Visible = no

iv. Then double check the manage apps page to verify that the app was created

splunk-enterprise

Apps

Administrator

Messages

Settings

Activity

Help

Find

Apps

Browse more apps

Install app from file

Create app

Showing 1-25 of 33 items

filter

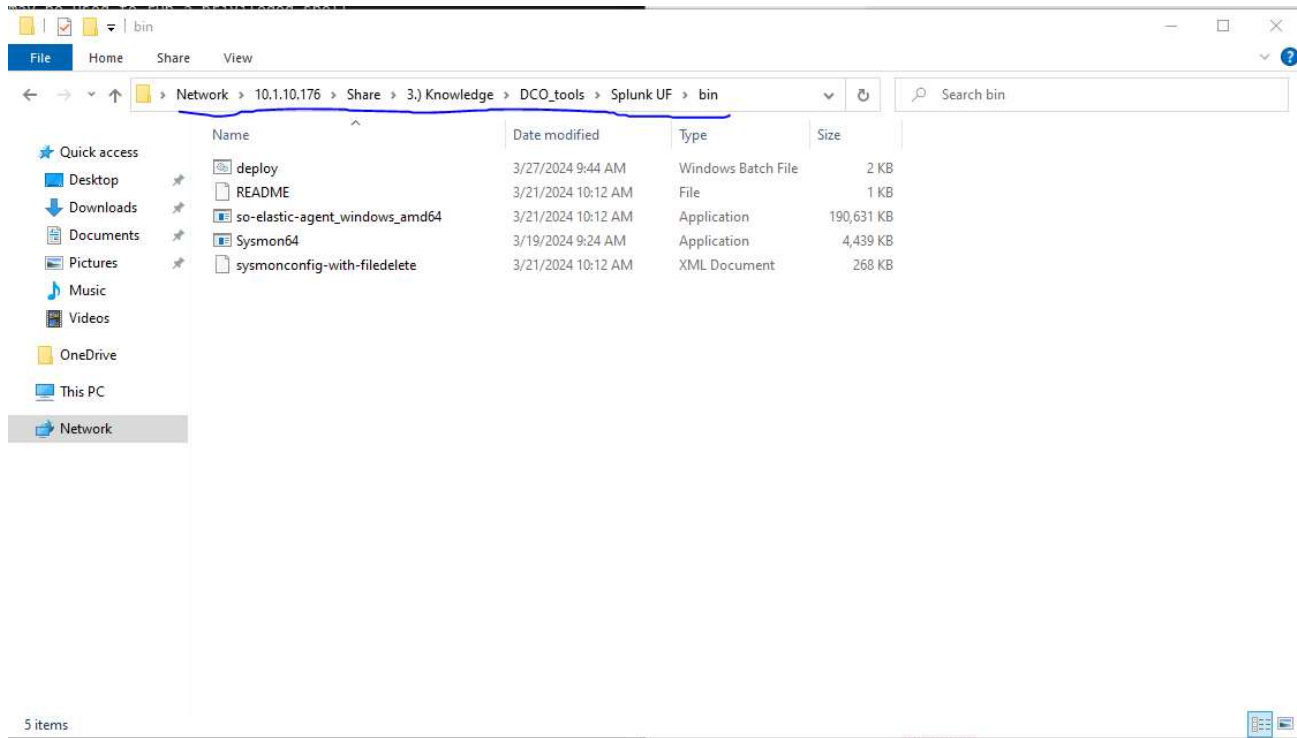
25 per page

Prev12Next

Name	Folder name	Version	Update checking	Visible	Sharing	Status	Actions
Corelight App For Splunk	CorelightForSplunk	2.4.6	Yes	Yes	Global Permissions	Enabled Disable	Launch app Edit properties View objects View details on Splunkbase
SplunkForwarder	SplunkForwarder		Yes	No	App Permissions	Disabled Enable	
SplunkLightForwarder	SplunkLightForwarder		Yes	No	App Permissions	Disabled Enable	
Splunk Add-on for Sysmon	Splunk_TA_microsoft_sysmon	3.1.0	Yes	No	Global Permissions	Enabled Disable	Edit properties View objects View details on Splunkbase
Splunk Add-on for Zeek	Splunk_TA_zeek	10.5	Yes	No	Global Permissions	Enabled Disable	Edit properties View objects View details on Splunkbase
TA-suricata-4	TA-suricata-4	2.3.4	Yes	No	Global Permissions	Enabled Disable	Edit properties View objects View details on Splunkbase
ThreatHunting	ThreatHunting	1.5.1	Yes	Yes	Global Permissions	Enabled Disable	Launch app Edit properties View objects View details on Splunkbase
Log Event Alert Action	alert_logevent	9.0.4.1	Yes	No	App Permissions	Enabled Disable	Edit properties View objects
Webhook Alert Action	alert_webhook	9.0.4.1	Yes	No	App Permissions	Enabled Disable	Edit properties View objects
Apps Browser	appsbrowser	9.0.4.1	Yes	No	App Permissions	Enabled	Edit properties View objects
DCO Tools	dco_tools	10.0	Yes	No	App Permissions	Enabled Disable	Edit properties View objects
introspection_generator_addon	introspection_generator_addon	9.0.4.1	Yes	No	App Permissions	Enabled Disable	Edit properties View objects
journal_input	journal_input		Yes	No	App Permissions	Enabled Disable	Edit properties View objects
Home	launcher		Yes	Yes	App Permissions	Enabled	Launch app Edit properties View objects
learned	learned		Yes	No	App Permissions	Enabled Disable	Edit properties View objects
legacy	legacy		Yes	No	App Permissions	Disabled Enable	
Upgrade Readiness App	python_upgrade_readiness_app	4.0.3	Yes	Yes	App Permissions	Enabled Disable	Launch app Edit properties View objects View details on Splunkbase
sample data	sample_app		Yes	No	App Permissions	Disabled Enable	
Search & Reporting	search	9.0.4.1	Yes	Yes	App Permissions	Enabled	Launch app Edit properties View objects
Splunk Dashboard Studio	splunk-dashboard-studio	17.4	Yes	Yes	App Permissions	Enabled Disable	Launch app Edit properties View objects
Splunk Archiver App	splunk_archiver	1.0	Yes	No	App Permissions	Enabled Disable	Edit properties View objects View details on Splunkbase
Splunk Assist	splunk_assist	10.3	No	No	App Permissions	Enabled Disable	Edit properties View objects View details on Splunkbase
	splunk_essentials_9_0	10.0	Yes	Yes	App Permissions	Enabled Disable	Launch app Edit properties View objects View details on Splunkbase

[https://30.110.72800/en-US/Cloud and Enterprise 9.0](#)

- 3) SSH into splunk cli using MobaXterm
 - a. Ip:30.1.10.72
 - b. Username: dco_admin
 - c. Password: Standard
- 4) ****First step is you are going to copy dco_tools from /opt/splunk/etc/apps to /opt/splunk/etc/deployment-apps****
 - a. Cd /opt/splunk/etc/apps
 - i. You need to run this command before running the command below
 - b. Sudo cp -r dco_tools /opt/splunk/etc/deployment-apps/
 - i. This should copy the dco_tools app to the deployment-apps directory
- 5) You will then Switch to the dco_tools copy in the deployment apps directory
 - a. Cd /opt/splunk/etc/deployment-apps/dco_tools
 - i. If the command does not run, run the command "sudo su" and then run the cd command again
 - b. When you use the "ls" command you should see 4 directories
 - i. Bin, default, local, and metadata
 - c. In the /opt/splunk/etc/deployment-apps/dco_tools/bin directory
 - i. Mv the deploy.bat , sysmon.exe , sysmonconfig-with-filedelete.xml , so-elastic-agent-windows_amd64.exe into this directory
 - 1) Ensure you know the location of the files before running, if you need the files, they are in the share in the file location below
 - 2) Copy the files over to your desktop and then make note of where they are



- 3) The command to mv the files over to the splunk cli is "mv (filepath of the file)"
 - a) Run this command individually for each file
 - i) The commands below are examples as to how the command should look
 - ii) `Mv /home/dco_admin/deploy.bat .`
 - iii) `Mv /home/dco_admin/sysmonconfig-with-filedelete.xml .`
 - iv) `Mv /home/dco_admin/sysmon64.exe .`
 - v) `Mv /home/dco_admin/so-elastic-agent_windows_amd64 .`
 - b) Modify the deploy.bat if need be
- d. In the default directory
 - i. Create file inputs.conf
 - 1) Sudo vim inputs.conf
 - a) -copy the text below into inputs.conf
 - i) `[script://.\bin\deploy.bat]`
`disabled = False`
`interval = 3600`
 - `[WinEventLog://Microsoft-Windows-Sysmon/Operational]`
`index= sysmon`
`sourcetype = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational`
`disabled = false`
`renderXml = true`
 - `[WinEventLog://Security]`
`disabled = false`
`index = win_security`
`sourcetype = wineventlog:Security`
`renderXml = false`
 - `[WinEventLog:System]`
`disabled = false`
`index = win_system`
`sourcetype = wineventlog:System`
`renderXml=false`
 - `[WinEventLog://Application]`
`disabled = false`
`index = win_application`
`sourcetype = wineventlog:Application`
`renderXml=false`
 - b) Once put in, it should look like the image below

```

[[script://.\\bin\\deploy.bat
disabled = False
interval = 3600

[WinEventLog://Microsoft-Windows-Sysmon/Operational]
index= sysmon
sourcetype = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational
disabled = false
renderXml = true

[WinEventLog://Security]
disabled = false
index = win_security
sourcetype = wineventlog:Security
renderXml = false

[WinEventLog://System]
disabled = false
index = win_system
sourcetype = wineventlog:System
renderXml=false

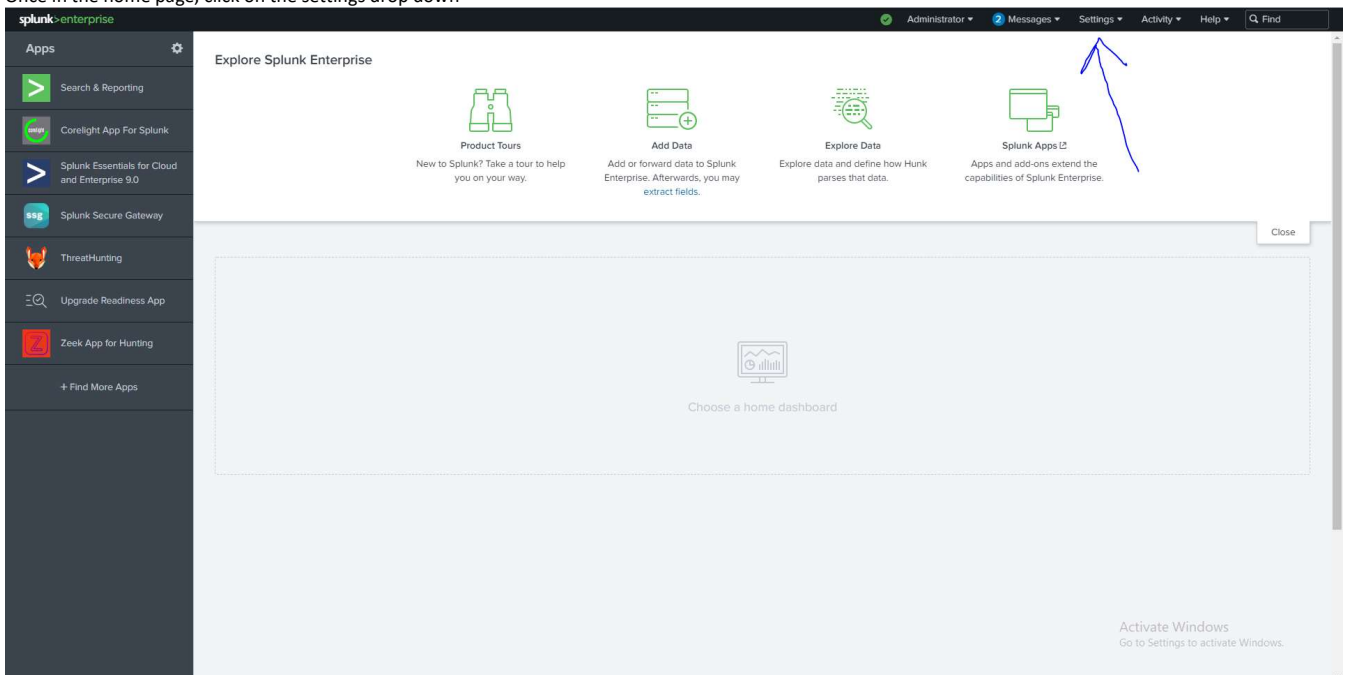
[WinEventLog://Application]
disabled = false
index = win_application
sourcetype = wineventlog:Application
renderXml=false

"inputs.conf" 28L, 576B

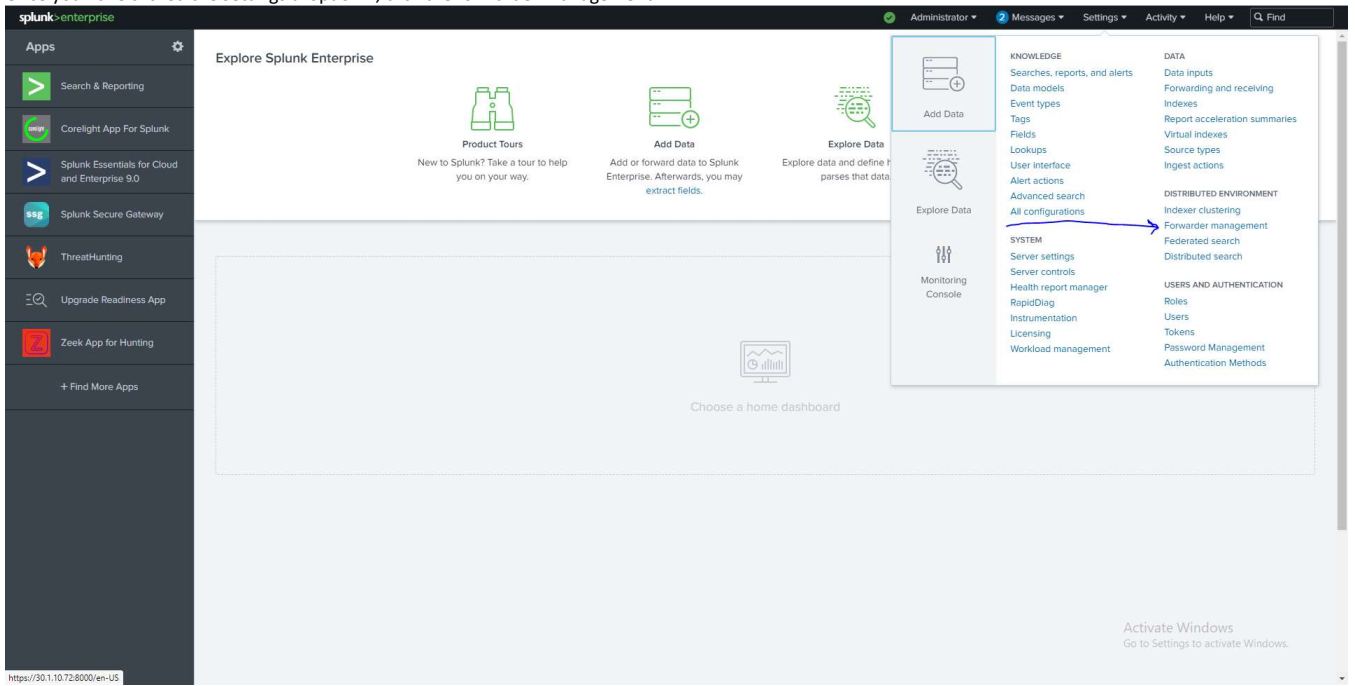
```

- ii. Reload the deployment server with the command below
 - 1) /opt/splunk/bin/splunk reload deploy-server

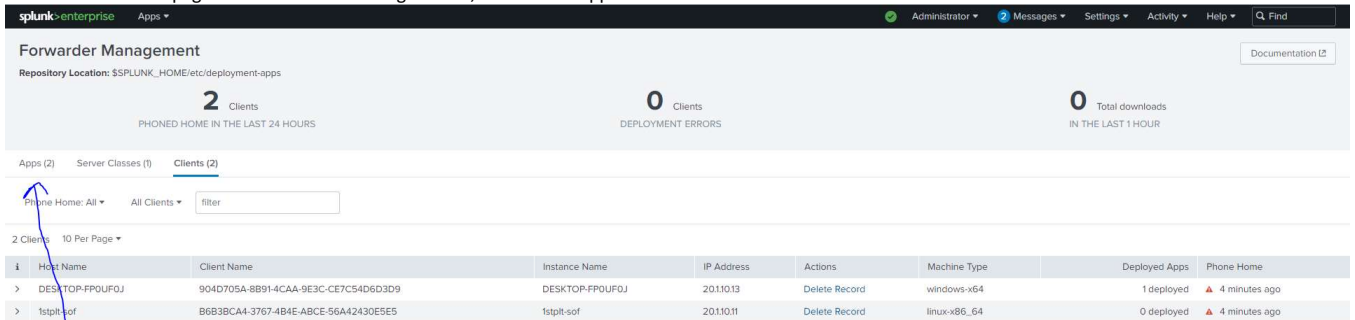
- 6) Once you the deployment server has been reloaded, go back to the Splunk webpage and verify the app is now up
 - a. Once in the home page, click on the settings drop down



- b. A
- c. Once you have clicked the settings dropdown, click the forwarder management



- d. A
- e. You will now be in a page that looks like the image below, click on the Apps tab



- f.
- g. A
- h. Once you click on the apps tab you should now be able to see the app that you created

splunk-enterprise Apps ▾ Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Forwarder Management

Repository Location: \$SPLUNK_HOME/etc/deployment-apps

2 Clients
PHONED HOME IN THE LAST 24 HOURS

0 Clients
DEPLOYMENT ERRORS

0 Total downloads
IN THE LAST 1 HOUR

Documentation

Apps (2) Server Classes (1) Clients (2)

Deployed Successfully ▾ filter

2 Apps 10 Per Page ▾

Name	Actions	After Installation	Clients
dco_tools	Edit ▾	Enable App	1 deployed
ToolDeployment	Edit	Enable App	0 deployed

Activate Windows
Go to Settings to activate Windows.

i.

j. You will then click on the edit button under the actions column

splunk-enterprise Apps ▾ Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Forwarder Management

Repository Location: \$SPLUNK_HOME/etc/deployment-apps

2 Clients
PHONED HOME IN THE LAST 24 HOURS

0 Clients
DEPLOYMENT ERRORS

0 Total downloads
IN THE LAST 1 HOUR

Documentation

Apps (2) Server Classes (1) Clients (2)

Deployed Successfully ▾ filter

2 Apps 10 Per Page ▾

Name	Actions	After Installation	Clients
dco_tools	Edit ▾	Enable App	1 deployed
ToolDeployment	Edit	Enable App	0 deployed

Activate Windows
Go to Settings to activate Windows.

https://30.1.10.72:8000/en-US

k.

l. A

m. Once you click on the edit button, you should be on a page that looks like the image below, you will then click the check box to enable "Restart Splunkd" and click save

Edit App: dco_tools Documentation

Server Classes

dco_tools x +

After Installation

☒ Enable App

☐ Restart Splunkd

Cancel **Save**

Phone Home: All All Clients filter

1 Clients 10 Per Page

Host Name	Client Name	Instance Name	IP Address	Actions	Machine Type	Deployed Apps	Phone Home
DESKTOP-FP0UF0J	904D705A-8B91-4CAA-9E3C-CE7C54D6D3D9	DESKTOP-FP0UF0J	2011013	Delete Record	windows-x64	1 deployed	3 minutes ago

Activate Windows
Go to Settings to activate Windows.

n.

7) In web interface, go to the server class tab and click create server class

splunk-enterprise Apps

Administrator Messages Settings Activity Help Find

Forwarder Management Documentation

Repository Location: \$SPLUNK_HOME/etc/deployment-apps

2 Clients
PHONED HOME IN THE LAST 24 HOURS

0 Clients
DEPLOYMENT ERRORS

0 Total downloads
IN THE LAST 1 HOUR

Apps (2) **Server Classes (1)** Clients (2)

All Server Classes filter

New Server Class

1 Server Classes 10 Per Page

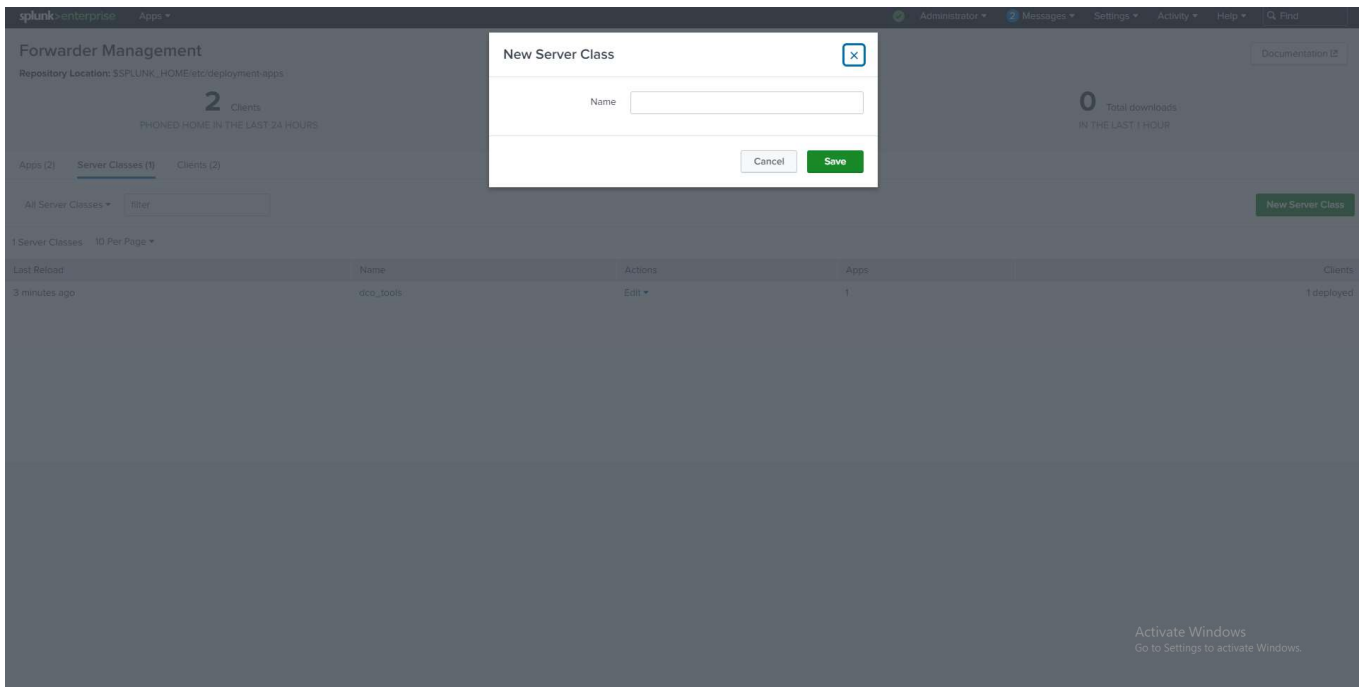
Last Reload	Name	Actions	Apps	Clients
3 minutes ago	dco_tools	Edit	1	1 deployed

Activate Windows
Go to Settings to activate Windows.

<https://30.110.72.8000/en-US>

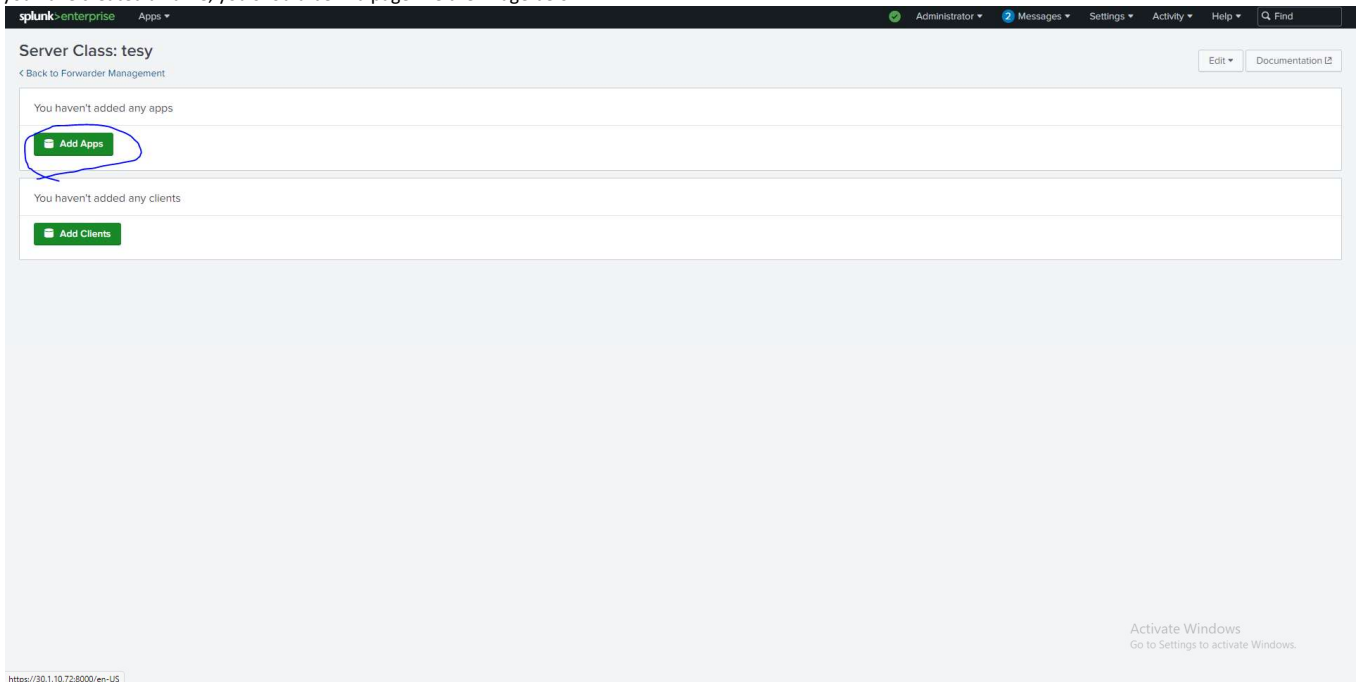
a.

8) Once you click to create a new server class, you will give it a name



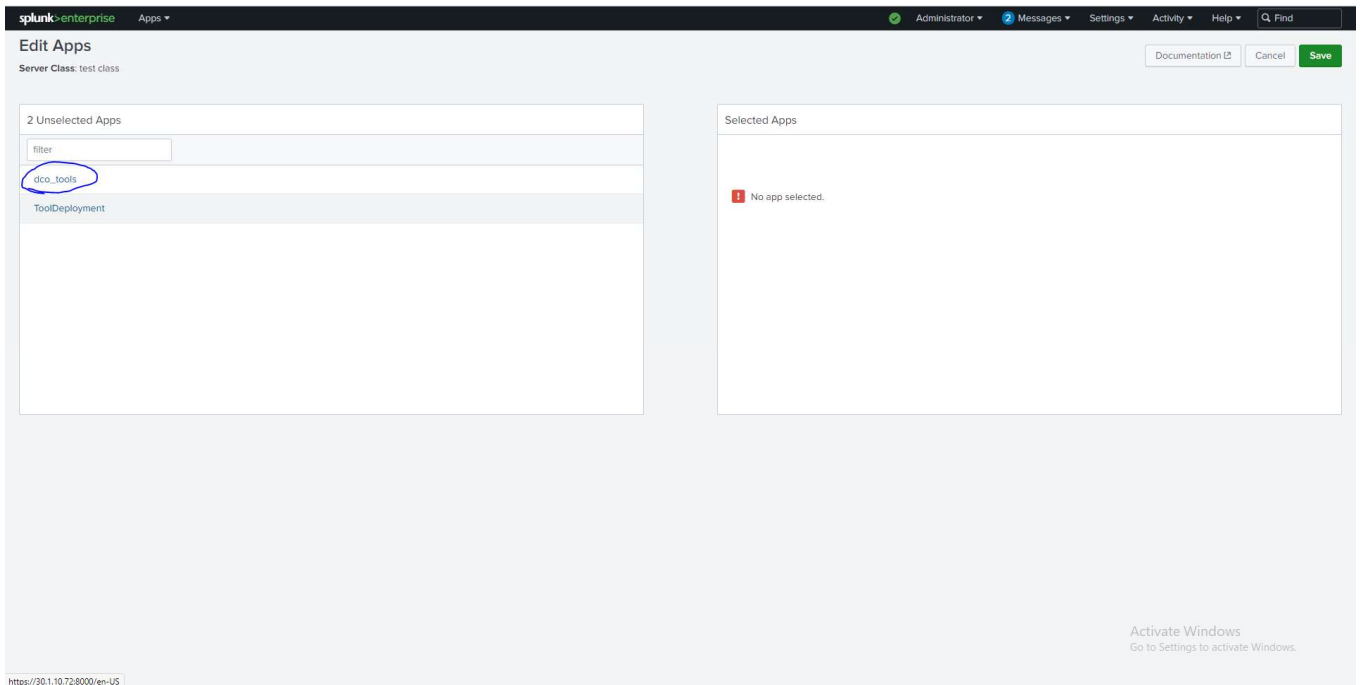
a.

9) Once you have created a name, you should be in a page like the image below



a.

10) Once you do click to add apps, you will click the app you created and save, you save, you will click "Go back to Forwarder Management" so you can verify the creation of the server class



a.

Edit server class and include "*"