## Splunk Forwarder (WINDOWS)

Thursday, March 28, 2024 12:18 PM

#### On the windows machine:

1) Install the forwarder onto the host



#### 2) On the Splunk webpage

a. Create an app

i	Once in the	Solunk webpage	go to the	manage apps n	age
1.	Unce in the		, go to the	manage apps p	age

splunk>enterprise			🥝 Admir	nistrator ▼ Messages ▼ Settings ▼	Activity • Help •	Q, Find
Apps 🗢 Explor	re Splunk Enterprise					
Search & Reporting	88					
Corelight App For Splunk	Li					
Splunk Essentials for Cloud	Product Tours New to Splunk? Take a tour to help	Add Data Add or forward data to Splunk	Explore Data Explore data and define how Hunk	Splunk Apps 12 Apps and add-ons extend the		
and Enterprise 9.0	you on your way.	Enterprise. Afterwards, you may extract fields.	parses that data.	capabilities of Splunk Enterprise.		
Splunk Secure Gateway						Close
ThreatHunting						
三〇 Upgrade Readiness App						
Zeek App for Hunting						
+ Find More Apos		(O I				
		Choose a hor	e dashboard			
https://30.1.10.72:8000/en-US/app/launcher/home#						

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

Apps							Browse more apps Install app from file
Showing 1-25 of 32 items							
filter Q							
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 Splunk
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   E View details on Splunkbase
Splunk Add-on for Zeek	Splunk_TA_zeek	1.0.5	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 Splunk
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 Splunk
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	1.7.4	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://30.1.10.72:8000/en-US loud 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 Splunk
vou click on "Croate Ann" v	ou will soo the image	holow					

Add new Apps > Add new		
Nam		
	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	n	
	App version.	
Visible	e 🔿 No 💌 Yes	
	Only apps with views should be made visible.	
Autho	Name of the app's owner.	
Description		
o campion		
	Enter a description for your app.	
Template	e barebones ·	
	Inese tempiates contain example views and searches.	
Upload asse	Can be any time is or other file to arid to your ann	
	den de uny nomi ja di duna, me la dadi la your oppo	
	Cancel Sove	

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

 a) Name = DCO Tools
 b) Foldername = dco\_tools

- c) Version = 1.0.0d) Visible = no

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

splunk>enterprise Apps •						0	Administrator • Messages • Settlings • Activity • Help • Find
Apps Showing 1-25 of 33 items							Browse more apps Install app from file Create app
filter							25 per page +
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   12 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   12 View details on Splunkbase
Splunk Add-on for Zeek	Splunk_TA_zeek	1.0.5	Yes	No	Global   Permissions	Enabled   Disable	Edit properties   View objects   전 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   12 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   12 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	1.7.4	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   [2] View details on Splunkbase
Splunk Assist	splunk_assist	1.0.3	No	No	App   Permissions	Enabled   Disable	Edit properties   View objects   Lt View details on Splunkbase
https://30.1.10.72:8000/en-US <sup>3</sup> loud and Enterprise 9.0	splunk_essentials_9_0	1.0.0	Yes	Yes	App   Permissions	Enabled   Disable	Launch app   Edit properties   View objects   [2] View details on Splunkbase

#### 3) SSH into splunk cli using MobaXterm

- a. lp:30.1.10.72
- b. Username: dco\_admin
- c. Password: Standard
- \*\*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 "Is" 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. My the deploy.bat , sysmon.exe , sysmonconfig-with-filedelete.xml , so-elastic-agentwindows\_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

Name	B				
	Date modified	Туре	Size		
log deploy	3/27/2024 9:44 AM	Windows Batch File	2 KB		
README	3/21/2024 10:12 AM	File	1 KB		
so-elastic-agent windows amd64	3/21/2024 10:12 AM	Application	190,631 KB		
III Sysmon64	3/19/2024 9:24 AM	Application	4,439 KB		
sysmonconfig-with-filedelete	3/21/2024 10:12 AM	XML Document	268 KB		
- 100 · · · · · · · · · · · · · · · · · ·					
	<ul> <li>deploy</li> <li>README</li> <li>so-elastic-agent_windows_amd64</li> <li>Sysmon64</li> <li>sysmonconfig-with-filedelete</li> </ul>	Image: System of System	Image: System of Control	Image: System of Control	Image: System of Control

- 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-filedelet.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

<pre>[script://.\\bin\\deploy.bat] disabled = False interval = 3600</pre>		
[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		
N N		
~		
N		
N N		
N N		
N		
~		
N		
~~ ~		
N		
N.		
N		
"inputs.conf" 28L, 576B	1,1	All

- ii. Reload the deployment server with the command below1) /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

а.	Once	in the home page	, click on the settings dro	p down					
	splunk	t>enterprise				🥝 Administi	ator 👻 🙎 Messages 👻 Settings	▪ Activity ▪ Help ▪ Q F	Find
	App	\$ <b>\$</b>	Explore Splunk Enterprise				$\wedge$	<b>`</b>	Î
	>	Search & Reporting		<u>ب</u>					
	(enter	Corelight App For Splunk		Product Tours	Add Data	Explore Data	Splunk Apps (2		
	>	Splunk Essentials for Cloud and Enterprise 9.0		New to Splunk? Take a tour to help you on your way.	Add or forward data to Splunk Enterprise. Afterwards, you may extract fields.	Explore data and define how Hunk parses that data.	Apps and add-ons extend the capabilities of Splunk Enterprise.		
	ssg	Splunk Secure Gateway							-
		ThreatHunting							Close
	ΞQ	Upgrade Readiness App							
		Zeek App for Hunting							
		+ Find More Apps							
								Activate WINDOWS Go to Settings to activate Wind	

	b.	A Once you have clicked	the settings drondown cli	ck the forwarder mana	agement					
<complex-block></complex-block>	с.	splunk>enterprise	ine settings aropaown, en		agement	0	Administrator 👻 💈	🛛 Messages 🔻 Settings 🕶 Acti	vity • Help • Q Find	
<complex-block></complex-block>		Apps 🌣				Г	_			1
<complex-block></complex-block>			Explore Splunk Enterprise					Searches, reports, and alerts	Data inputs	
<complex-block></complex-block>		Search & Reporting		<u>L</u>				Data models Event types	Forwarding and receiving Indexes	
		Corelight App For Splunk			(+)		Add Data	Tags Fields	Report acceleration summaries Virtual indexes	
		Solunk Essentials for Cloud		Product Tours New to Splunk? Take a tour to help	Add Data Add or forward data to Splunk	Explore Data Explore data and define h		Lookups User interface	Source types	
		and Enterprise 9.0		you on your way.	Enterprise. Afterwards, you may extract fields.	parses that data		Alert actions	DISTRIBUTED ENVIRONMENT	
I de la constante de la con		Splunk Secure Gateway					Explore Data	All configurations	Indexer clustering	
		1.4					616	SYSTEM	Federated search	
		ThreatHunting					I9I Monitoring	Server controls	Distributed search	
		ΞQ Upgrade Readiness App					Console	Health report manager RapidDiag	Roles	
		<b>(</b>						Instrumentation Licensing	Users Tokens	
<pre>**** Note day</pre>		Zeek App for Hunting						Workload management	Password Management Authentication Methods	
Choose a hone deabloard Activate Windows Cit St Cit Strates and States and		+ Find More Apps								
c. 4. c. 4 c. 4 c. 5 c. 5 c. 6. 4 c. 6. 4 c. 6. 1 <pc. 1<="" 6.="" p=""> c. 6. 1 c.</pc.>										
At the second										
c. A c. A c. A c. A c. Sum now be not block like the image below, click on the Apps table c. Market Windows Market W										
A definition of the second region of the second										
e. A le										
expense is a service with the service is a serv										
A characterized in the second of the seco										
d. A c. A Construction of the page that looks like the image below, click on the Apps table <b>Construction of the page that looks like the image below, click on the Apps table <b>Construction of the page that looks like the image below, click on the Apps table <b>Construction of the page that looks like the image below, click on the Apps table <b>Construction of the page that looks like the image below, click on the Apps table <b>Construction of the page that looks like the image below, click on the Apps table <b>Construction of the page that looks like the image below, click on the Apps table <b>Construction of the page that looks like the image below, click on the Apps table <b>Construction of the page the page that looks like the image below, click on the Apps table <b>Construction of the page the page the page the page the page table <b>Construction of the page the page the page table <b>Construction of the page the page the page table <b>Construction of the page the page table </b></b></b></b></b></b></b></b></b></b></b></b>										
<pre>d. d. A A A A A A A A A A A A A A A A A A A</pre>								Go to Se	ttings to activate Windows.	
d. A e. Sum on the page that looks like the image below, click on the Apps the  <		https://30.1.10.72:8000/en-US								
e. You will now be in a page that looks like the image below, click on the Apps tables and tab	d.	A								
Spand Control (1) Append (1)     Point Control (1) <td>e.</td> <td>You will now be in a pa</td> <td>ge that looks like the imag</td> <td>e below, click on the A</td> <td>Apps tab</td> <td></td> <td>A destate and a second</td> <td></td> <td></td> <td></td>	e.	You will now be in a pa	ge that looks like the imag	e below, click on the A	Apps tab		A destate and a second			
		spiunk>enterprise Apps •				0	Administrator •	Messages     Settings     Acti	Mity + Help + C Fina	
Implementation       Implementation       Implementation       Implementation       Implementation         Appe (2)       Server Classes (1)       Clients (2)       Encomment (2)		Forwarder Managemer	1t atc/denloyment.anns						Documentati	on 🖾
Clients Clients   HONED HOME IN THE LAST 24 HOURS DEPLOYMENT ERRORS     Apps (2) Server Classes (1) Clients (2)   Phone Home: All  All Clients (2)     2 Clients 10 Per Page *     1 Hot Name   2 Diest TOP-PPOUFOJ 9040705A 88914-CAA-9E3C-CE7C54050309   2 DESKTOP-FPOUFOJ 2011013   2 Dest TOP-PPOUFOJ 9040705A 88914-CAA-9E3C-CE7C54050309   2 Istipht of BB63BCAA-3767/4B4E-ABCE-56A42430E5E5     1 Hot Name IP Address Actions Machine Type Deployed Apps Phone Home   f.		Reported ported to the rome.	<b>2</b>		0			0		
Apps (2)       Server Classes (1)       Clients (2)         Prove Home: All        All Clients *       Iter         2. Clients       10 Per Page *       Iter Name       Client Name       Instance Name       IP Address       Actions       Machine Type       Deployed Apps       Phone Home         2. DES: TOP. FPOUFDJ       9040705A & B914CAA 9E3C-CE7C54050309       DE5KTOP.FPOUFDJ       2011013       Delete Record       windows x64       1 deployed A 4 minutes ago         3       tspth of       B683BCA4-37074B4E-ABCE-56A42430E5E5       tspth sof       2011011       Delete Record       Inux-x86_64       0 deployed A 4 minutes ago         f.            0 deployed A 4 minutes ago       4 minutes ago		PHONED HO	Clients OME IN THE LAST 24 HOURS		DEPLOYMENT ERRORS			IN THE LAST 1 HOUR	5	
Aprx (2) Server Classes (1) Clients (2)  Phone Home: All · All Clients · Iller  2. Clients 10 Per Page * <u>1 Hot Name</u> Client Name Instance Name IP Address Actions Machine Type Deployed Apps Phone Home 2. DES\TOP-FPOUFDJ 2011013 Delete Record windows x64 1 deployed A 4 minutes ago 3 tsph of B638CA4-3767/484E-ABCE-56A42430E5E5 tsph of 2011011 Delete Record Insux-86_64 0 deployed A 4 minutes ago f.										
Physice Home: All · All Clients · Iller         2. Clients       10 Per Page *         1       Hot Name       Client Name       Instance Name       IP Address       Actions       Machine Type       Deployed Apps       Phone Home         2. DES TOP-FPOUFDJ       90.40705A-8891-4CAA-9E3C-CE7C54060309       DESKTOP-FPOUFDJ       20.10.13       Delete Record       windows-x64       1 deployed A 4 minutes ago         2       tsph-of       B6838CA4-3767-484E-ABCE-56A42430E5E5       tsph-of       20.10.11       Delete Record       Inux-x86_64       0 deployed A 4 minutes ago		Apps (2) Server Classes (1) Clie	nts (2)							
2. Clinets       10 Per Page *         i       Hort Name       Client Name       Instance Name       IP Address       Actions       Machine Type       Deployed Apps       Phone Home         >       DESLTOP.FPOUF0J       20.10.13       Delete Record       windows-x64       1 deployed A 4 minutes ago         >       tsiph-of       B633BCA4-3767-484E-ABCE-56A42430E5E5       tsiph-of       20.10.11       Delete Record       Inu-x86_64       0 deployed A 4 minutes ago		Phone Home: All - All Clients -	filter							
Instance Name       Client Name       Client Name       Instance Name       IP Address       Actions       Machine Type       Deployed Apps       Phone Home         i       DES/T0P.FPOUFDJ       904D705A.48914/CAA.9E3C-CE7C54D603D9       DES/T0P.FPOUFDJ       201013       Delete Record       windows-x64       1 deployed A_4 minutes apa         i       tsph-of       B6336CA4-3767-484E-ABCE-56A42430E5E5       tsph-sof       201011       Delete Record       Imux-x86_64       0 deployed A_4 minutes apa         f.             4 minutes apa		2 Clients 10 Per Page •								
b DESKTOP-FPOUFOJ 904D705A-8891-4CAA-9E3C-CE7C54D6D3D9 DESKTOP-FPOUFOJ 2011013 Delete Record window:s64 1 deployed A 4 minutes ago b tsph-of B6838CA4-3767-484E-ABCE-56A42430E5E5 tstph-sof 2011011 Delete Record linux:x86_64 0 deployed A 4 minutes ago		i Host Name	Client Name	Instance 1	Name IP Address	Actions	Machine Type	Deployed	Apps Phone Home	
> tstptt of B6B3BCA4-3767-484E-ABCE-56A42430E5E5 tstptt-sof 20.110.11 Delete Record linux-x86_64 O deployed A 4 minutes ago		> DESCTOP-FPOUFOJ	904D705A-8B91-4CAA-9E3C-CE7C54D6D3D9	DESKTOP	P-FPOUF0J 20.1.10.13	Delete Record	windows-x64	1 dep	oloyed 🔺 4 minutes ago	
f. \		> 1stplt-sof	B6B3BCA4-3767-4B4E-ABCE-56A42430E5E5	1stplt-sof	20.1.10.11	Delete Record	linux-x86_64	0 dep	oloyed 🔺 4 minutes ago	
,	f.									

# https://30.1.10.72:8000/en-US

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 •	2 Messages 🔻	Settings 🕶	Activity -	Help -	Q. Find
Forwarder Management Repository Location: \$SPLUNK_HOME/etc/deployment-apps								Documentation 년
2 Clients PHONED HOME IN THE LAST 24 HOURS		Clients DEPLOYMENT ERRORS		1	Total dow	nloads OUR		
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

i.

Activate Windows Go to Settings to activate Windows. j. You will then click on the edit button under the actions column splunk-enterprise Apps\* Porwarder Management Repository Location: SSPUINK-HOME/enterprise 2 cliens PHONED HOME IN THE LAST 24 HOURS DEPLOYMENT ERRORS DEPLOYMENT ERRORS NTHE LAST 1 HOUR

Deployed Successfully • filter	Apps (2) Server Classes (1) Clients (2)			
	Deployed Successfully • filter			
2 Apps 10 Per Page +	2 Apps 10 Per Page *			
Name Actions After Installation Clife	Name	Actions	After Installation	Clients
dco_tools Edit • Enable App 1deplo	dco_tools	Edit	Enable App	1 deployed
ToolDeployment Edit Enable App 0 deplo	ToolDeployment	Edit	Enable App	0 deployed

k.



https://30.1.10.72:8000/en-US

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

							Documentatio
Server Classes			After Installation				
dco_tools x +			Enable App				
		(	Restart Splunkd				
							Cancel
Phone Home: All - All Clients -	▼ filter						
1 Clients 10 Per Page 🕶							
i Host Name	Client Name	Instance Name	IP Address	Actions	Machine Type	Deployed Apps	Phone Home
> DESKTOP-FPOUF0J	904D705A-8B91-4CAA-9E3C-CE7C54D6D3D9	DESKTOP-FP0UF0J	20.1.10.13	Delete Record	windows-x64	1 deployed	A 3 minutes ago

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

	splunk>enterprise Apps •			🥝 Administrator 🔻 🌘	2) Messages ▼ Settings ▼ Activity ▼ Hel	lp ▼ Q. Find
	Forwarder Management Repository Location: \$SPLUNK_HOME/etc/deployment-apps					Documentation 12
	2 Clients PHONED HOME IN THE LAST 24 HOURS		Clients DEPLOYMENT ERRORS		Total downloads	
	Apps (2) Server Classes (1) Clients (2)					
	All Server Classes filter					New Server Class
	1 Server Classes 0 Per Page 🔻					71
	Last Reload	Name	Actions	Apps		Clients
	3 minutes ago	dco_tools	Edit •	1	/	1 deployed
a.						
					Activate Windo Go to Settings to act	WS ivate Windows.
	https://30.1.10.72:8000/en-US					

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

splunk>enterprise Apps *			Ø Administrator	* 2 Messages * Settings * Activity * Help * Q. Find
Forwarder Management Repository Location: SSPLUNK_HOME/etc/deployment-app	1	New Server Class	×	
2 Clients PHONED HOME IN THE LAST 2/	4 HOURS	Name		O Total downloads IN THE LAST I HOUR
		с	ancel Save	
				New Server Class

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

se Apps *	Maministrator •	🧭 messages 🔹 Setuni	Js • Activity •	Help •	C4 Find
s: tesy				Edit •	Documentation
Ided any apps					
ided any clients					
15					
			Activate W		
-US					

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

