

Elastic Agent

Friday, August 23, 2024 9:12 AM

Download the elastic agent from online, not from the downloads page from security onion.
Unzip the folder and place in splunk in your deployment app.



elastic-agent
t-8.10.4-...

(here is the 8.10.4 zip of the elastic agent)

```
root@splunk:/opt/splunk/etc/deployment-apps/dco_tools/bin# ls  
deploy.bat elastic-agent-8.10.4-windows-x86_64 README Sysmon64.exe sysmonconfig-with-filedelete.xml
```

(here is where that unzip file goes in splunk)

Now go to Fleet in security onion > go to settings tab.
For Fleet Server Host, select add fleet server and make it your external IP. Make it default.

Fleet server hosts

Specify the URLs that your agents will use to connect to a Fleet Server. If multiple URLs exist, Fleet will show the first provided URL for enrollment purposes. For more information, see the [Fleet and Elastic Agent Guide](#).

Name	Host URLs	Default	Actions
grid-default	https://30.1.10.64:8220		
	https://kaiser-som:8220		
External_FLEET	https://172.22.1.3:8220	✓	

[+ Add Fleet Server](#)

For Outputs, go to security onion CLI and stop the logstash service
Sudo so-logstash-stop
Click on the the pencil for grid-logstash and add a host (your external IP)

Outputs

Specify where agents will send data.

Name	Type	Hosts	Default	Actions
grid-logstash	logstash	30.1.10.64:5055		
		kaiser-som:5055	Agent integrations	
		172.22.1.3:5055	Agent monitoring	
default	Elasticsearch	http://localhost:9200		
so-manager_elasticsearch	Elasticsearch	https://kaiser-som:9200		

Start the Logstash service in security onion
Sudo so-logstash-start

Make changes to the deploy.dat in splunk as needed

```
if "%ElasticAgentStatus%"==" " (  
  cd %ElasticAgentDir%  
  .\elastic-agent.exe install --insecure --force --url=https://172.22.1.3:8220 --enrollment-token=SG5yMmRaRUJHS19wZHo4LWttbV  
A60UJQ5zM4RkdSV3lHeXRkV1laV0tGUQ=  
  net start 'Elastic Agent'
```

Here is an example of what would be in the deploy.bat (change the enrollment key to what is in your security onion, this is found in add agent > select endpoint initial > go to windows and the shown command will be present with the right enrollment key)