


## Atomicorp Enterprise Ossec Getting Started

### Pre-launch:

1. Ensure that traffic is allowed on ports 22 and 30000 for either this instance or all instances. Go to the GCP VPC network section and then to firewall rules. Select create a firewall rule and create an ingress rule for tcp ports 22, 80, 443, 1515 and 30000 and udp ports 1514 and 514. Also create an egress rule for the same ports if one doesn't already exist.

### Example:

 Your free trial is waiting: activate now to get \$300 credit to explore Google Cloud products. [Learn more](#)

Google Cloud Platform Atomicorp-public

VPC network Firewall rules [CREATE FIREWALL RULE](#) [REFRESH](#) [DELETE](#)

VPC networks  
External IP addresses  
**Firewall rules**  
Routes  
VPC network peering  
Shared VPC  
Serverless VPC access

Firewall rules control incoming or outgoing traffic to an instance. By default, incoming traffic from outside your network is blocked. [Learn more](#)  
Note: App Engine firewalls are managed [here](#).

Filter resources Columns

<input type="checkbox"/>	Name	Type	Targets	Filters	Protocols / ports	Action	Priority	Network ^
<input type="checkbox"/>	aeo-outbound-rule	Egress	Apply to all	IP ranges: 0.0.0.0/0	all	Allow	1	default
<input type="checkbox"/>	aeo-inbound-rule	Ingress	Apply to all	IP ranges: 0.0.0.0/0	tcp:22,80,443,30000,1515 udp:1514,514	Allow	1	default
<input type="checkbox"/>	awp-firewall-rule2	Ingress	Apply to all	IP ranges: 0.0.0.0/0	tcp:22,30000	Allow	1	default

### Post-launch:

1. Upon starting the instance, wait approximately 15 minutes for background updates and scans to finish. If you have connected to the instance via ssh, you'll a line that says Atomic Endpoint Defender: Scan complete when it is finished. You may not see this if you wait till the scan is finished before connecting. Once this is done, follow the onscreen instructions. Only run the useradd command once unless you want to add more users. You can run the command asl by itself to see options for the asl command.

```
morganadavis95@awp-get-screenshot2~ - Google Chrome
ssh.cloud.google.com/projects/atomicorp-public/zones/us-east4-c/instances/awp-get-screenshot2?authuser=0&hl=en_US&projectNu...

agencies, both domestic and foreign.

By using this system, the user consents to such interception, monitoring,
recording, copying, auditing, inspection, and disclosure at the
discretion of such personnel or officials. Unauthorized or improper use
of this system may result in civil and criminal penalties and
administrative or disciplinary action, as appropriate. By continuing to
use this system you indicate your awareness of and consent to these terms
and conditions of use. LOG OFF IMMEDIATELY if you do not agree to the
conditions stated in this warning.
*****

Connected, host fingerprint: ssh-rsa 0 E8:13:BD:41:9A:BC:2A:BB:38:A3:2F:B9:56:B3
:AA:86:19:49:F6:73:19:FF:37:A4:AD:CD:C3:54:94:BD:90:04
#####
# Atomic Workload Protection v5.0 #
#####
To finish setup to access the console on https://<IP>:30000

Run the following:
sudo /var/asl/bin/asl-web-useradd

Go to https://<external_ip>:30000 to access the web ui.
[morganadavis95@awp-get-screenshot2 ~]$
Broadcast message from root@awp-get-screenshot2 (Thu Sep 26 15:15:04 2019):

Atomic Endpoint Defender: Scan complete

[morganadavis95@awp-get-screenshot2 ~]$
```

Example:

2. In order to connect an agent to the hub, run: `wget`  
[http://ip\\_of\\_hub/installers/ossec-installer.sh](http://ip_of_hub/installers/ossec-installer.sh) replacing `ip_of_hub` with the external ip of your instance.