

02. AWS SecOnion Lab Setup - Post Instance Configuration

AWS SecOnion Lab Setup - Post Instance Configuration

Click on instance and go to the connect tab (if you are unfamiliar with the setup)

The screenshot shows the AWS Management Console interface for an EC2 instance. The breadcrumb navigation at the top reads 'EC2 > Instances > i-07416c7b3d0a75a09'. Below this, the 'Instance details' tab is active, displaying the 'Instance summary for i-07416c7b3d0a75a09 (SecOnion)'. The summary indicates the instance was updated 'less than a minute ago'. A row of buttons includes a refresh icon, a 'Connect' button (highlighted with a red box), an 'Instance state' dropdown, and an 'Actions' dropdown. The instance details are organized into a grid:

Instance ID i-07416c7b3d0a75a09 (SecOnion) (highlighted with a red box)	Public IPv4 address 44.219.46.44 open address	Private IPv4 addresses 10.0.6.30 10.0.1.106
IPv6 address -	Instance state Running (with a green checkmark icon)	Public IPv4 DNS ec2-44-219-46-44.compute-1.amazonaws.com open address
Hostname type IP name: ip-10-0-1-106.ec2.internal	Private IP DNS name (IPv4 only) ip-10-0-1-106.ec2.internal	Elastic IP addresses
Answer private resource DNS name	Instance type	

Take note of any information there:

The user name is typically there, but for Security onion the user name is "onion"

As soon as you log in you'll be greeted with the setup:

Change the .pem key before attempting to log in:

```
chmod 400 S0Project.pem
```

Login:

```
ssh -i S0Project.pem onion@44.219.46.44
```

Security Onion Setup - 2.4.110

Welcome to Security Onion Setup!

You can use Setup for several different use cases, from a small standalone installation to a large distributed deployment for your enterprise. You can learn more in the documentation at:
<https://docs.securityonion.net/en/2.4>

Setup uses keyboard navigation and you can use arrow keys to move around. Certain screens may provide a list and ask you to select one or more items from that list. You can use the Space bar to select items and the Enter key to proceed to the next screen.

Would you like to continue?

<Yes>

<No>

Security Onion Setup - 2.4.110

What kind of installation would you like to do?

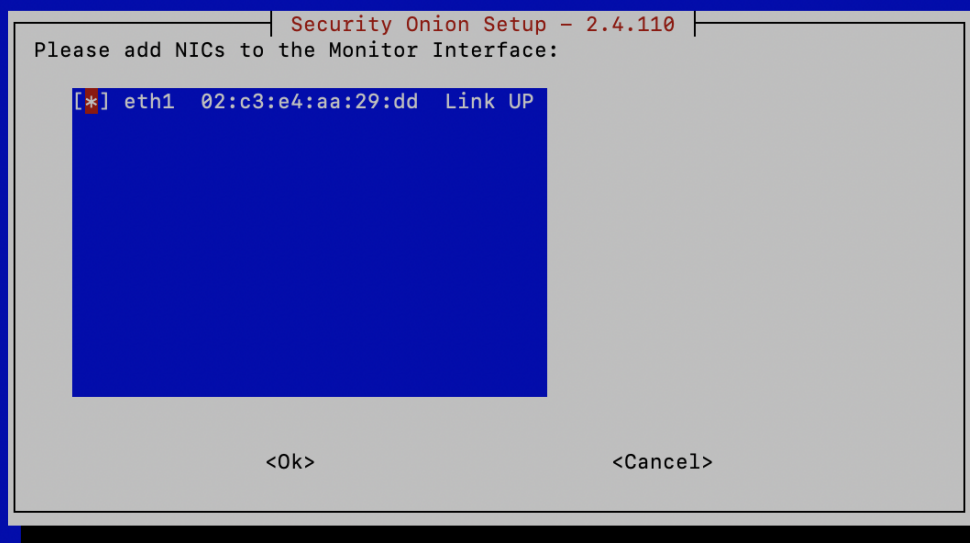
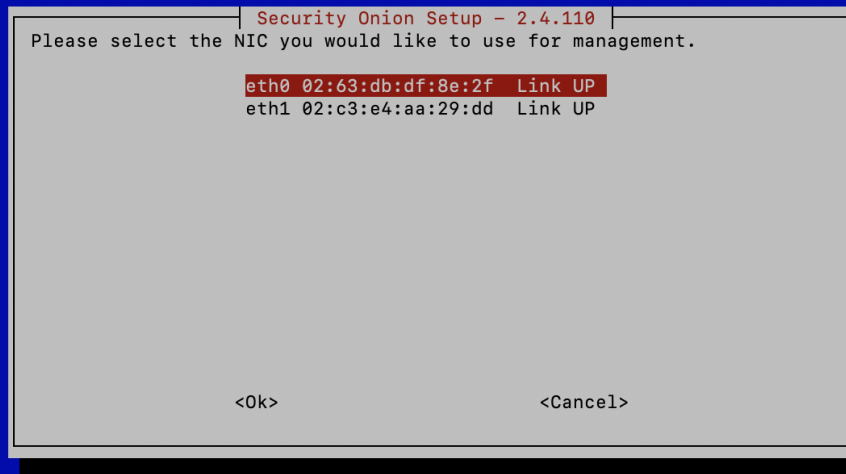
For more information, please see:

<https://docs.securityonion.net/en/2.4/architecture.html>

IMPORT	Import PCAP or log files
EVAL	Evaluation mode (not for production)
STANDALONE	Standalone production install
DISTRIBUTED	Distributed deployment
DESKTOP	Security Onion Desktop

<Ok>

<Cancel>



Email Address: arcpb@sos.com

Security Onion Setup - 2.4.110

Please enter an email address to create an administrator account for the Security Onion Console (SOC) web interface.

This will also be used for Elasticsearch and Kibana.

Must only include letters, numbers, or + - _ % . @ characters. All capitalized letters will be converted to lowercase.

arcps@sos.com

<Ok> <Cancel>

Setup should take 30-40 minutes:

Security Onion Setup - 2.4.110

STANDALONE setup is now complete!

Access the Security Onion Console (SOC) web interface by navigating to:
<https://projectso>

Then login with the following username and password.

SOC Username: arcps@sos.com
SOC Password: Use the password that was entered during setup

Press TAB and then the ENTER key to exit this screen.

<Ok>

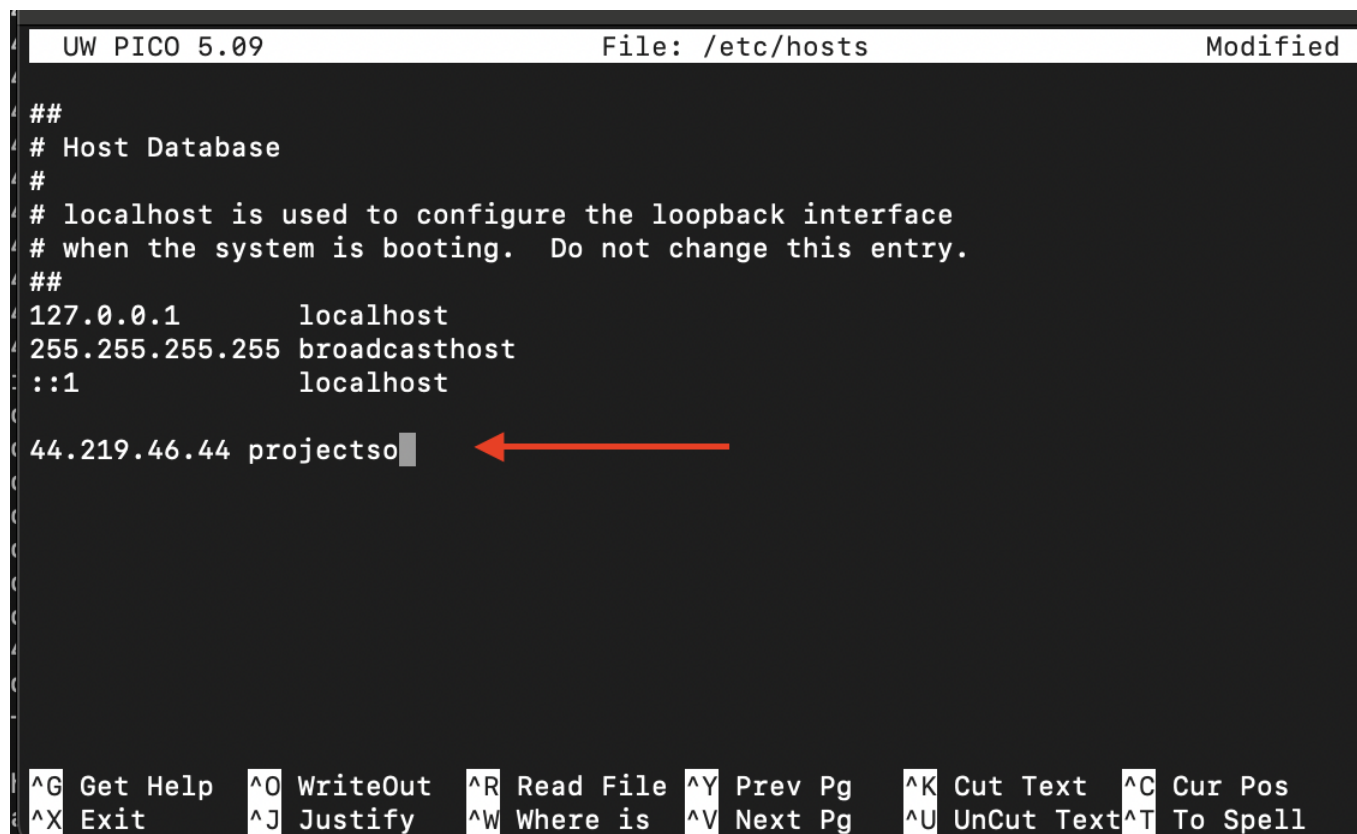
Optional

Add the ip / hostname to the /etc/hosts file

Linux/Unix -- /etc/hosts

Windows -- C:\Windows\System32\Drivers\etc\hosts

```
UW PICO 5.09      File: /etc/hosts      Modified
##
# Host Database
#
# localhost is used to configure the loopback interface
# when the system is booting. Do not change this entry.
##
127.0.0.1          localhost
255.255.255.255    broadcasthost
::1               localhost
44.219.46.44 projectso
```



Changing GUI password in the CLI

If you forget the password you set up you can reset it in the cli

`sudo so-user password --email unionuser@example.com cli` to reset password

Example: In the security onion cli

`sudo so-user (your_new_password_here) --email your-soc@email.com`

Example: In the security onion cli

```
sudo so-user P@ssw0rd1234 --email arcps@sos.com
```

Hostname to projectso (All Lowercase)