SAMSUNG

Samsung Wireless Enterprise

WES (Wireless Enterprise Security) Installation Manual

March 2015

Contents

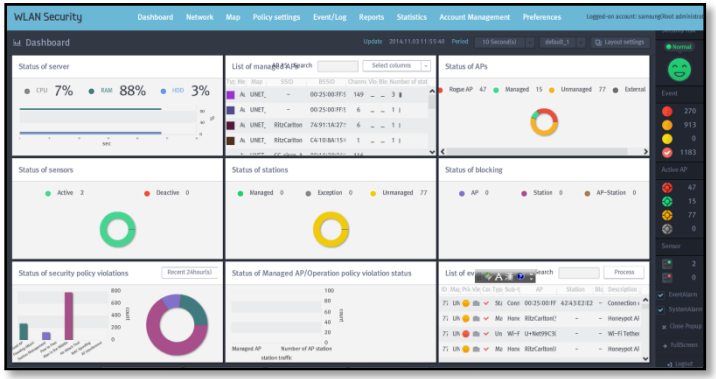
01

WES Features Overview

1.1 Features

1.2 Hardware & Software

The Samsung Wireless Enterprise Security (WES) product is a software tool for detecting, blocking and managing threats and attacks on an enterprise class WLAN. WES provides device classification, threat detection, monitoring, attack containment, forensic reporting, and additional WLAN performance management features available via a web-based GUI.



<u>The following is a quick overview of the main features of WES</u>:

Device Classification

The Samsung WES monitors the RF environment of your Enterprise in order to identify any devices that are interacting or attempting to interact with the WLAN. The system allows for the detection of all kinds of wireless devices using the standard protocols of 802.11a/b/g/n/ac and detects ranges of 2.4 GHz and 5 GHz bandwidths simultaneously. The WES classifies all wireless devices into groups whereby operational policies can be applied. Employing event, security, and operational policies, the WES can effectively manage and secure enterprise wireless services.

Item	Classifications
Access Points	Managed / Unmanaged / Rogue / Neighbor
User Stations	Managed / Unmanaged / Rogue / Temporary
Device Info	MAC / Vendor / SSID / Rogue / RSSI (Signal Strength)

Intrusion & Air Attack Detection

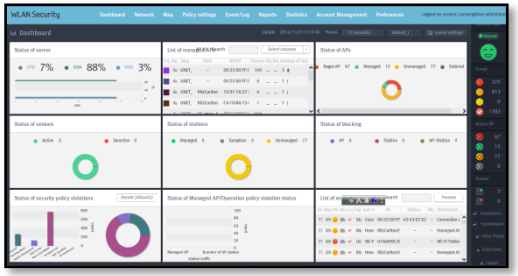
The Samsung WES can cope with a number of wireless security threats, prevent internal information leakages, and avoid security-related accidents before they affect the WLAN. WES can detect intentional network intrusions such as rogue AP's, MAC-spoofing AP's or stations, and ad-hoc devices. The WES system also detects a large amount of air attacks and identifies possible vulnerabilities:

Attack Type	WES Detection Types
Network Intrusion	Rogue AP's / MAC Spoofing AP's and Stations / Ad-hoc Devices
Denial of Service	Association / Disassociation / Authentication / Deauthentication Broadcasting / PS-Poll / Probe Request / RTS / CTS / EAPOL
RF Jamming	Microwave / Bluetooth / Wireless Video / Zigbee / Unknown Interference
Specific Attacks	Man in the Middle / Honeypot / WEP Cracking / AP Flooding
Vulnerabilities	Mismatched AP's and Stations / Hotspot AP via Cellular / WiFi Direct Mismatched Encryption Types, Authentications, Data Rates Wrong or Hidden SSID's

Threat Containment

In addition to detecting threats the WES system also contains them quickly in real time. Employing configurable automatic and manual containment rules and policies, WES can react to threats as they happen.

Forensics & Location Tracking



WES provides an at-a-glance dashboard to view important information on the status of servers, wireless devices, and even policy violations. The dashboard puts the functions of network logging, statistics, and reports at the fingertips of system administrators and managers.

Using custom uploaded floor plans, the WES system allows location tracking of both legitimate network events as well as unplanned network activity. RF environment data can be seen overlaid upon the network floorplan in order to pinpoint the location of wireless threats as well as normal network activities.

WLAN Performance Management

The WES assists in overall WLAN performance management for your network, either alone or interconnected to your current APC and/or WEM. By detecting misconfigured or vulnerable areas of your network, the WES system provides the ability to control the communication volume and operation policies of your WLAN via location and/or threshold based policies. Such information can also be used as supplementary data for enhancing the performance of networks in the future, managing the life-cycle of traffic in devices, and can serve as a traffic monitoring tool for checking trends in traffic changes.

Minimum WES Server Hardware Requirements

WES Server	Item	Minimum System Requirements
WES Sensors up to Qty: 200 (License required)	CPU	INTEL Pentium 1403v2 2.60 GHz
	MEM	8 GByte
	HDD	1 TByte
	Interface	1 GBps × 2, USB × 2, VGA, Console
	Power Supply	Dual Hot Plug Power Supplies 350W
WES Sensors up to Qty: 500 (License required)	CPU	INTEL Xeon E5-1410v2 2.80 GHz
	MEM	16 GByte
	HDD	1 TByte x 2, RAID
	Interface	1 GBps × 2, USB × 2, VGA, Console
	Power Supply	Dual Hot Plug Power Supplies 350W

Compatible Samsung APC and AP software versions

APC Model	AP Controller Software	Access Points 3xx	Access Points 4xx
WEC8500 Controller	wec8500_2.4.12R	weafama_2.4.12R	weafamb_2.4.12R
WEC8050 Controller	wec8050_2.4.12R	weafama_2.4.12R	weafamb_2.4.12R

02

Installation of WES Products

2.1 Server

2.2 Sensor

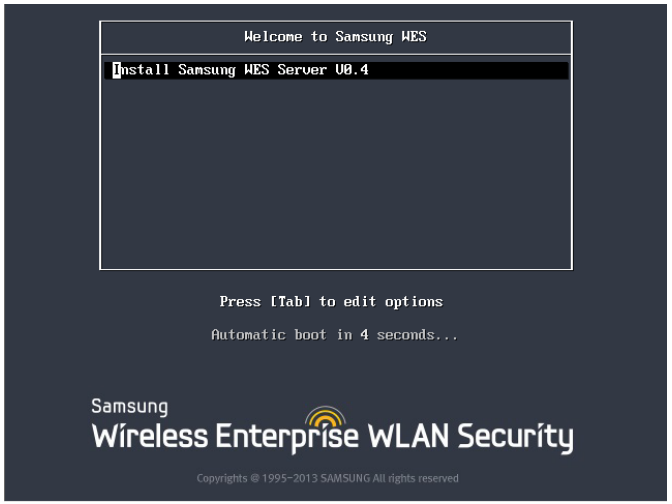
2.3 Network Ports

2.4 Administrator GUI

2.1 Server

2.1 Server

1. Insert and boot the server with the installation CD-ROM
2. When the OS selection screen is displayed, select "Install Samsung WES Server". *Note: the install will run automatically after a delay if the option is not physically selected.
3. The install process will complete automatically and shutdown the server after installation is complete.
4. After tuning on Server Power, remove the installation CD-ROM.
5. Use the following login and password to reach the server setup utility:
   Login: samsung
   Password: samsung
6. Complete the above process for the standby server if using High Availability mode.



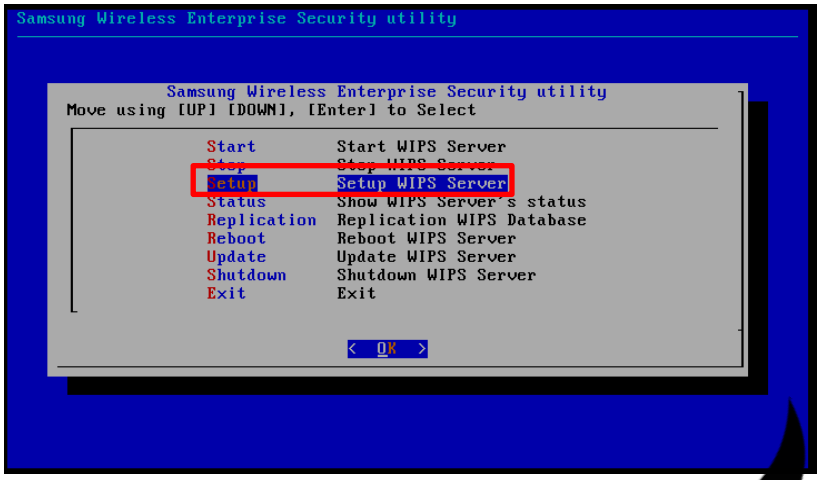
2.1.1 Standalone Server

2.1.1 Standalone Server

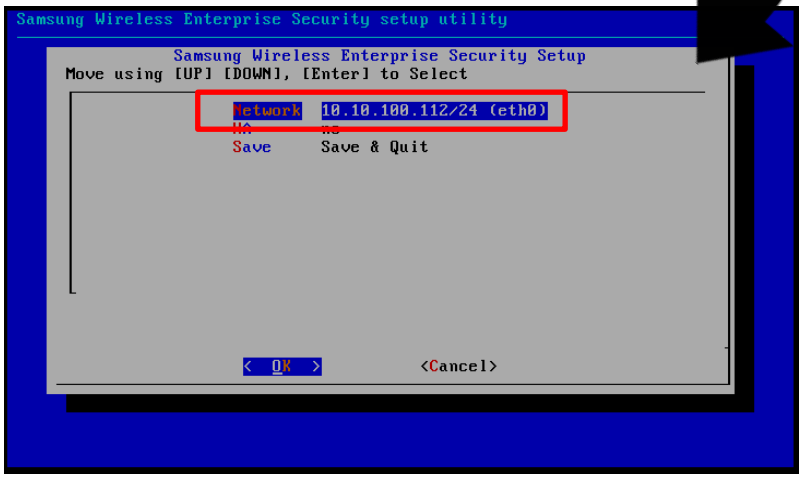
Use the following instructions to configure the WES in a single Standalone server mode.

If configuring High Availability (Active/Standby) mode, skip to section 2.1.2: High Availability Server

- **Select “Setup WIPS Server”**

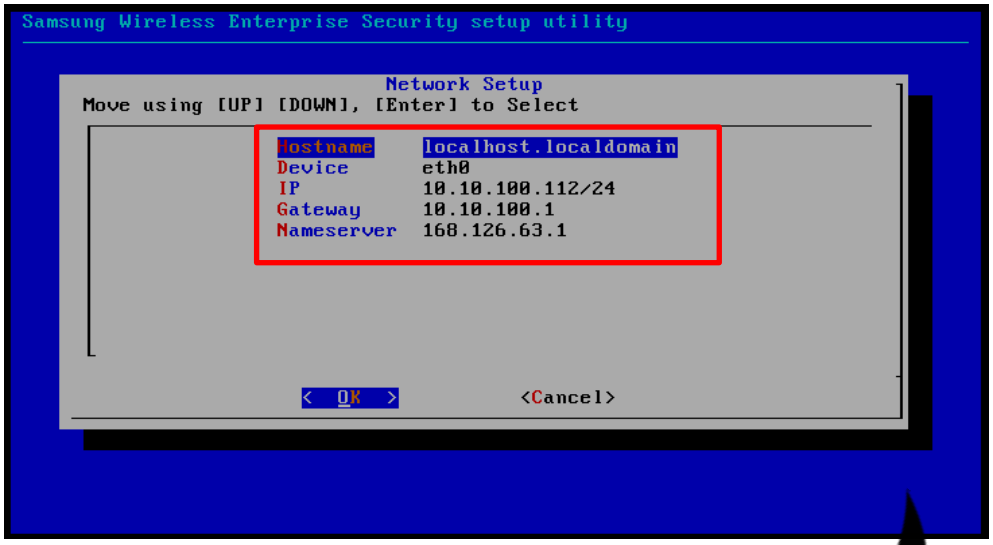


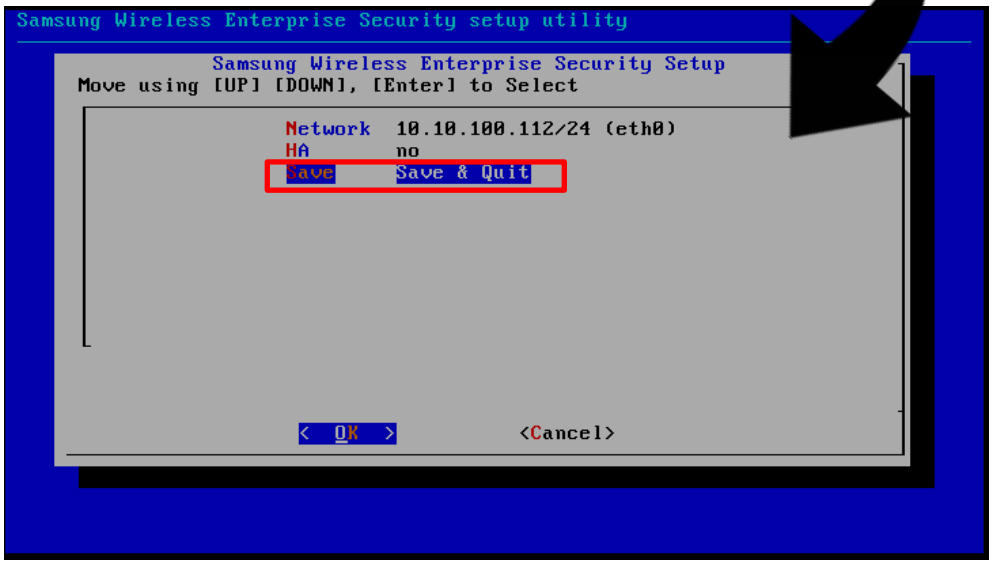
- **Select “Network”**



2.1.1 Standalone Server

Select and enter each of the items.
- Hostname (Enter Hostname)
- Device (Enter Network device name(eth0, em1 etc.)
- IP (Enter Server IP address)
- Gateway (Enter Gateway address)
- Nameserver (Enter DNS address)

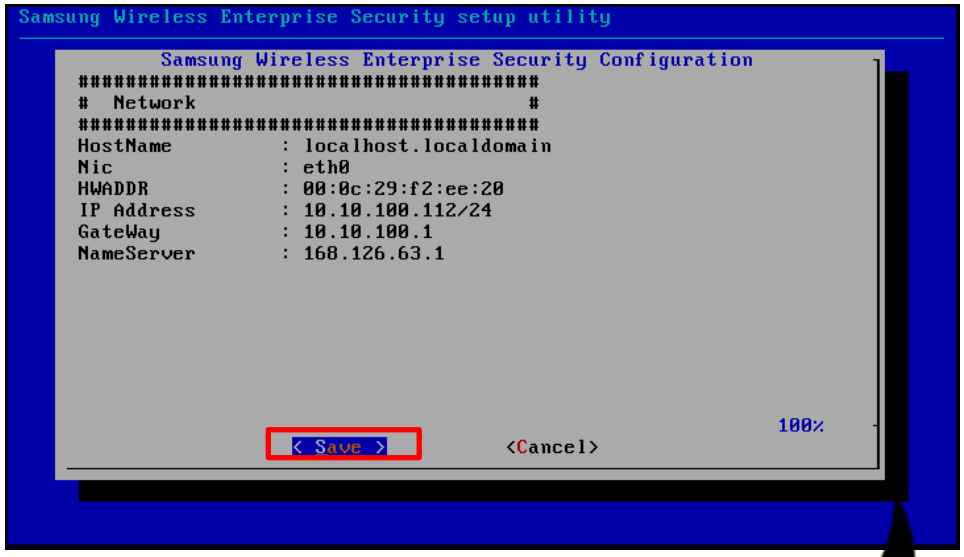




- To apply settings, select 'Save & Quit'

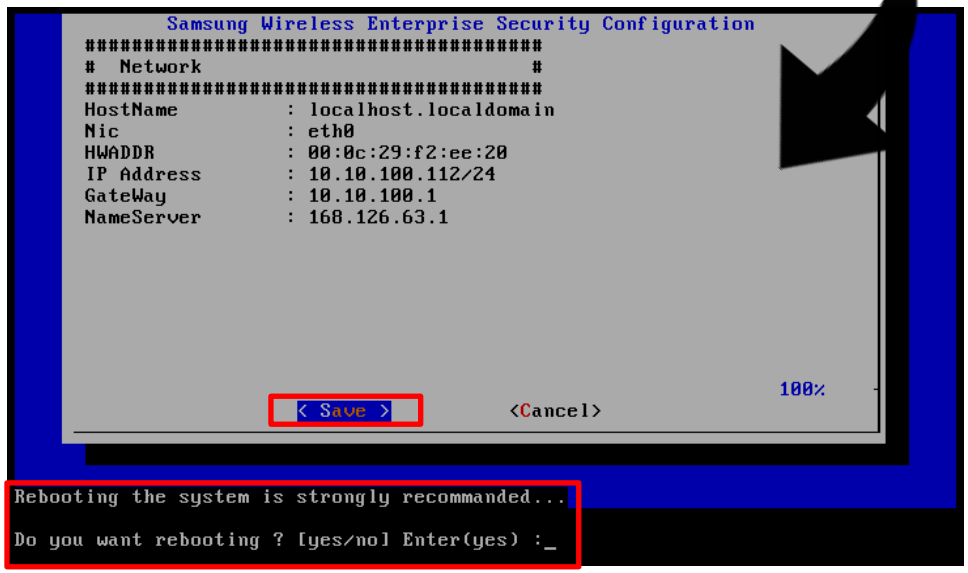
2.1.1 Standalone Server

Verify the settings entered and select ‘Save’



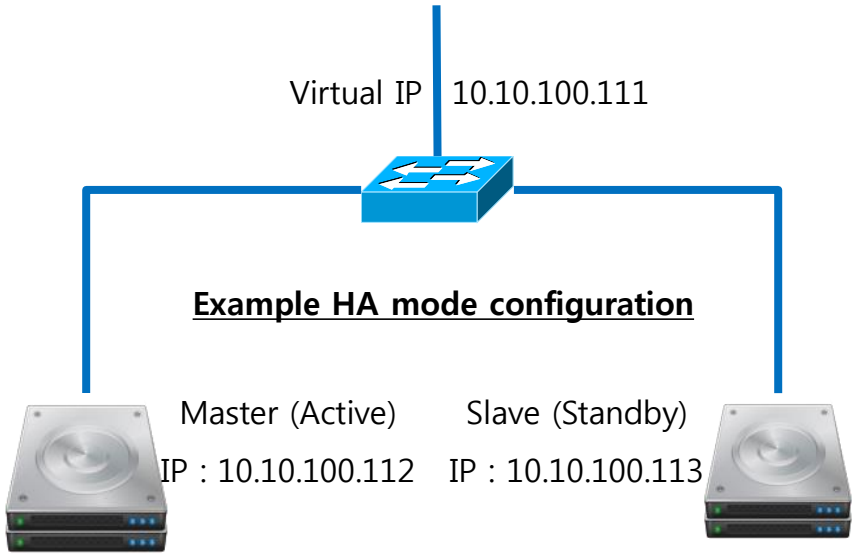
Type ‘Yes’ to reboot the server in order to complete the configuration.

Your server will reboot into the normal WES operating mode.



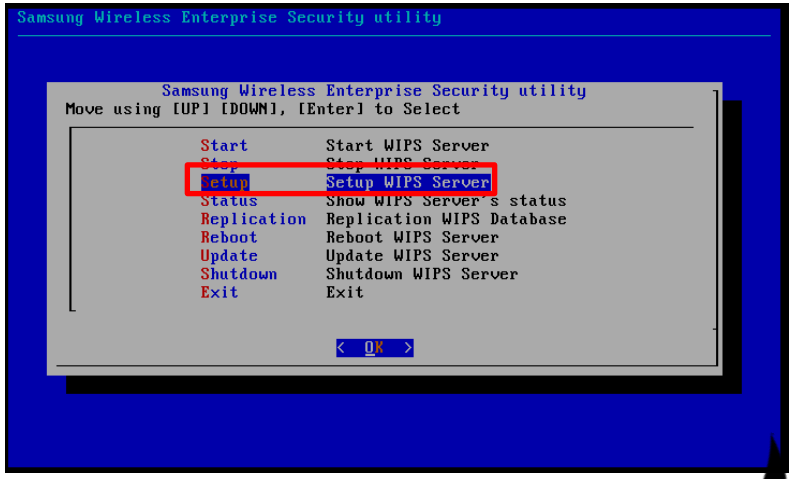
2.1.2 High Availability Servers

2.1.2 High Availability Servers

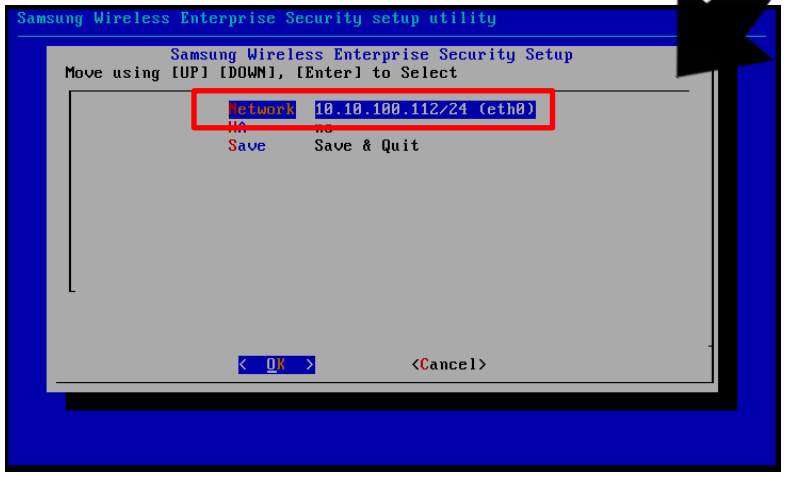


How to configure servers for High Availability Mode:

- **Perform these setup steps on both servers.**

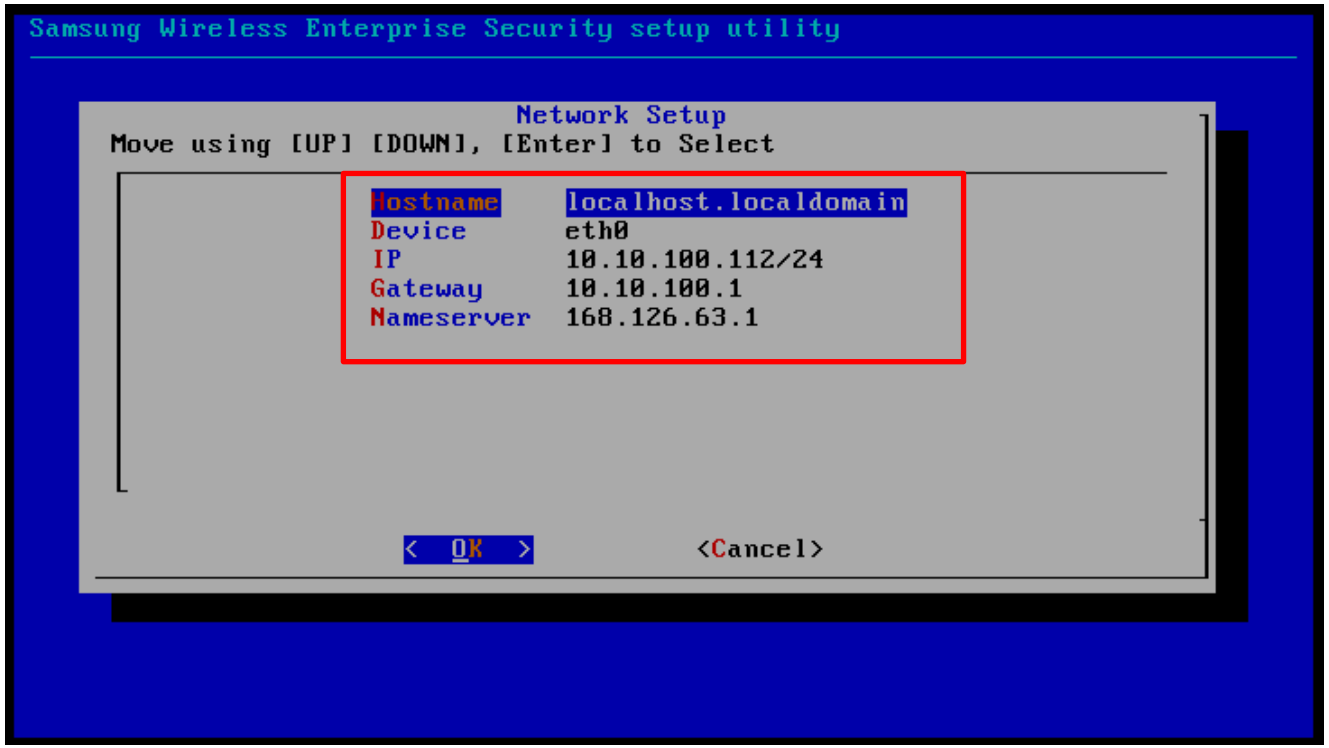


- **Select “Setup WIPS Server”**



- **Select “Network”**

2.1.2 High Availability Servers



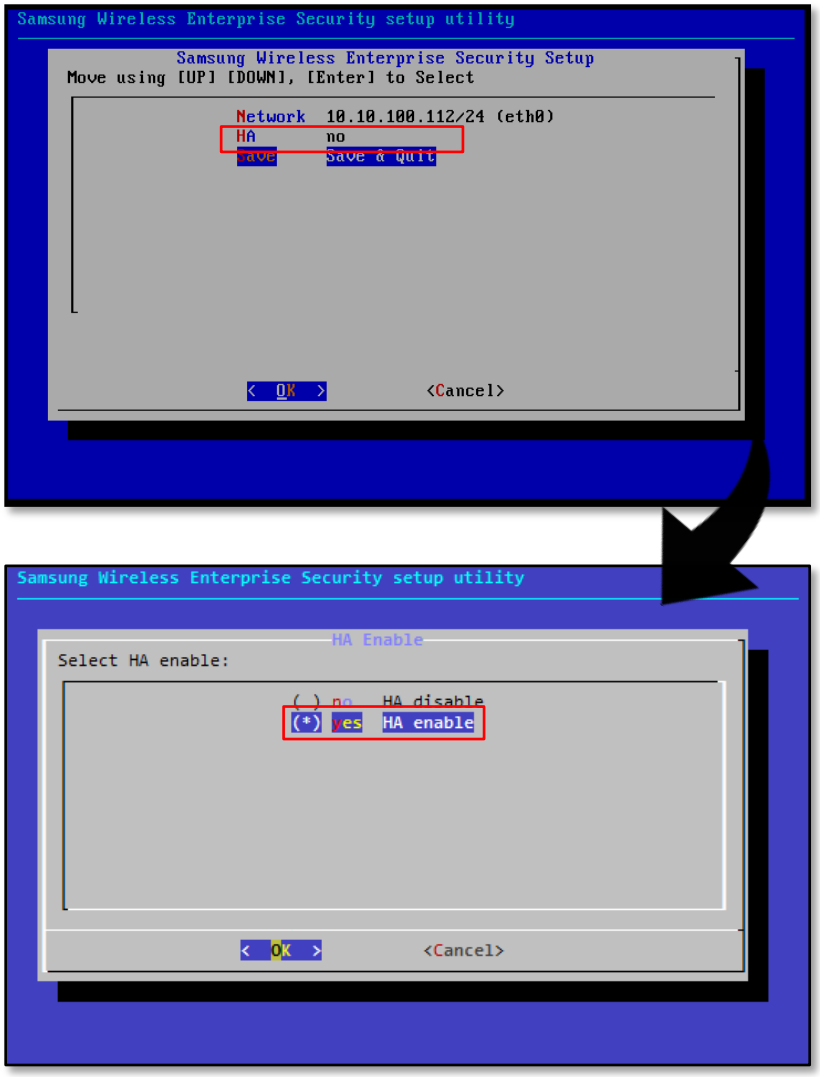
Select and enter each of the items.

- Hostname (Enter Hostname)
- Device (Enter Network device name(eth0, em1 etc.)
- IP (Enter Server IP address)
- Gateway (Enter Gateway address)
- Nameserver (Enter DNS address)

2.1.2 High Availability Servers

How to configure servers for High Availability Mode:

- **Perform these setup steps on both servers.**



- **Select ‘HA’**

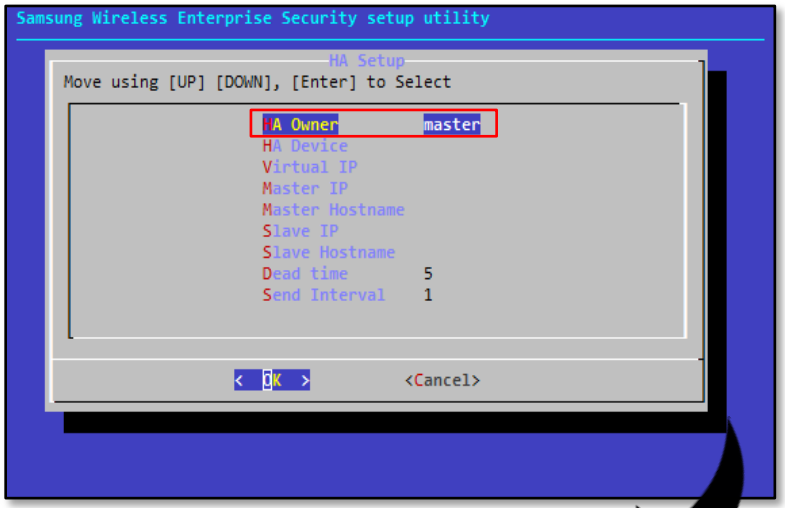
- **Select ‘Yes’.**
- **Arrow keys move up and down, and space bar selects the item.**

2.1.2 High Availability Servers

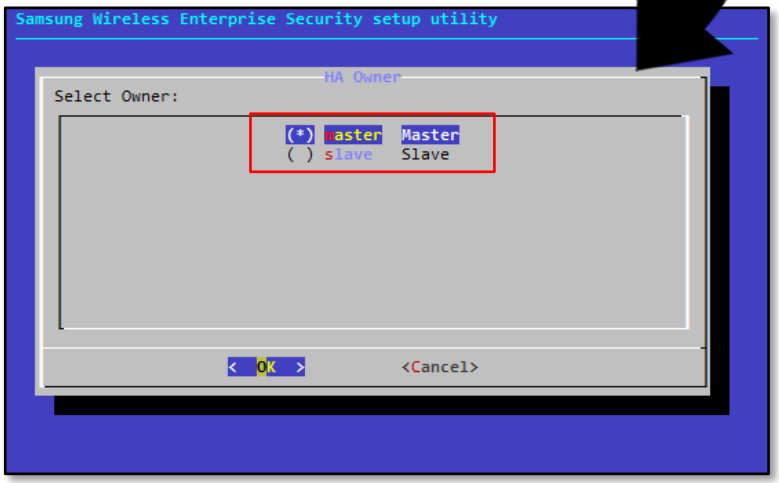
How to configure servers for High Availability Mode:

- **Perform these setup steps on both servers.**

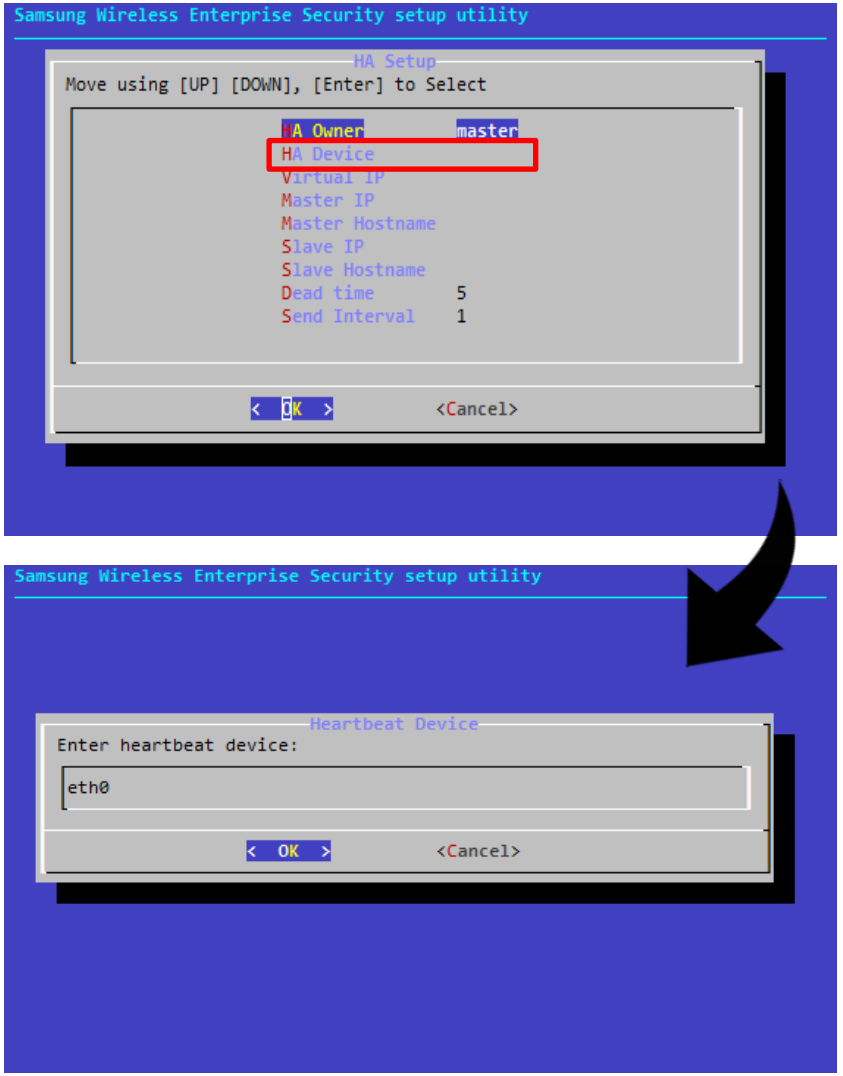
- **Select 'HA Owner'.**



- **Select the type for the server you are currently configuring.**
- **Arrow keys move up and down, and space bar selects the item.**



2.1.2 High Availability Servers



How to configure servers for High Availability Mode:

- **Perform these setup steps on both servers.**

- **Select 'HA Device'.**

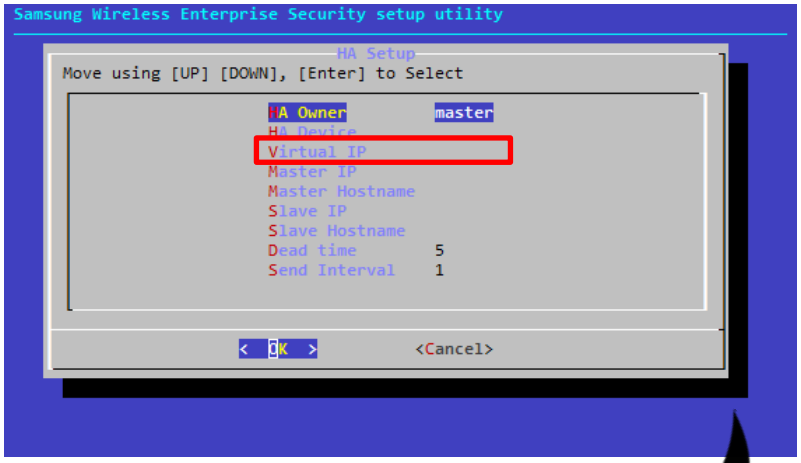
- **Enter Network device name (eth0, eth1 …etc.) which will transmit HA heartbeat message.**

2.1.2 High Availability Servers

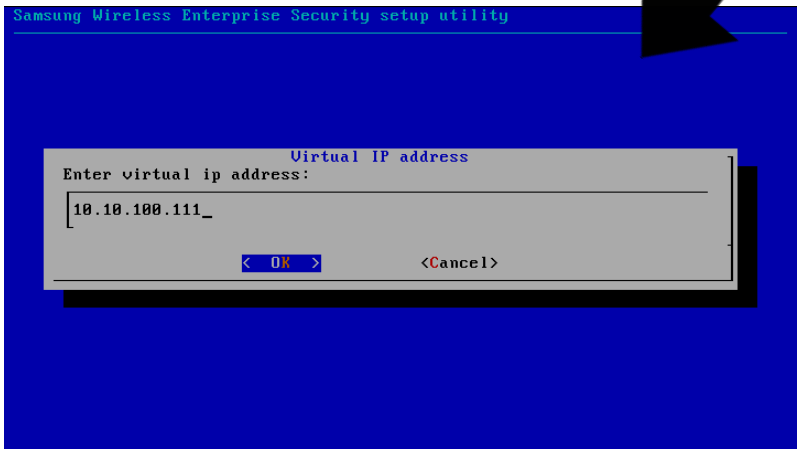
How to configure servers for High Availability Mode:

- **Perform these setup steps on both servers.**

- **Select ‘Virtual IP’.**



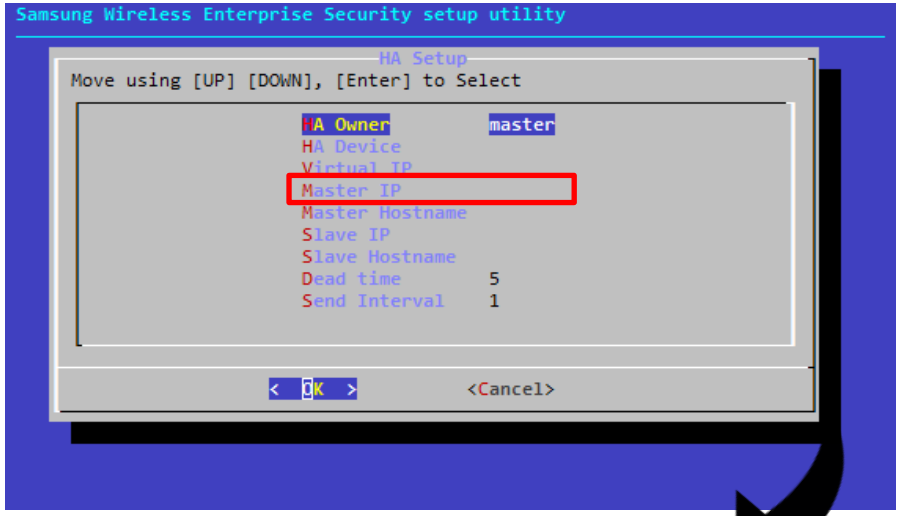
- **Enter the Virtual IP address that will be used to access via the administrator GUI.**



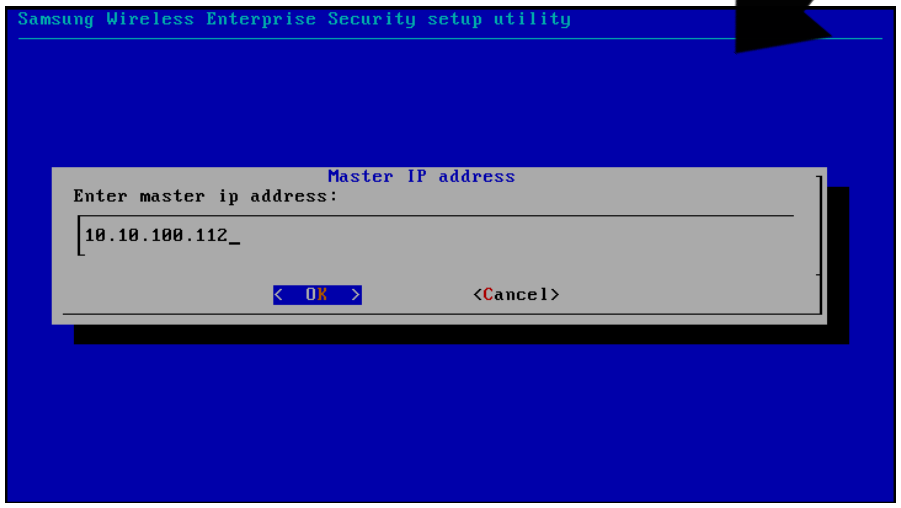
2.1.2 High Availability Servers

How to configure servers for High Availability Mode:

- **Perform these setup steps on both servers.**



- **Select 'Master IP'.**



- **Enter IP address of the Master (Active) server**

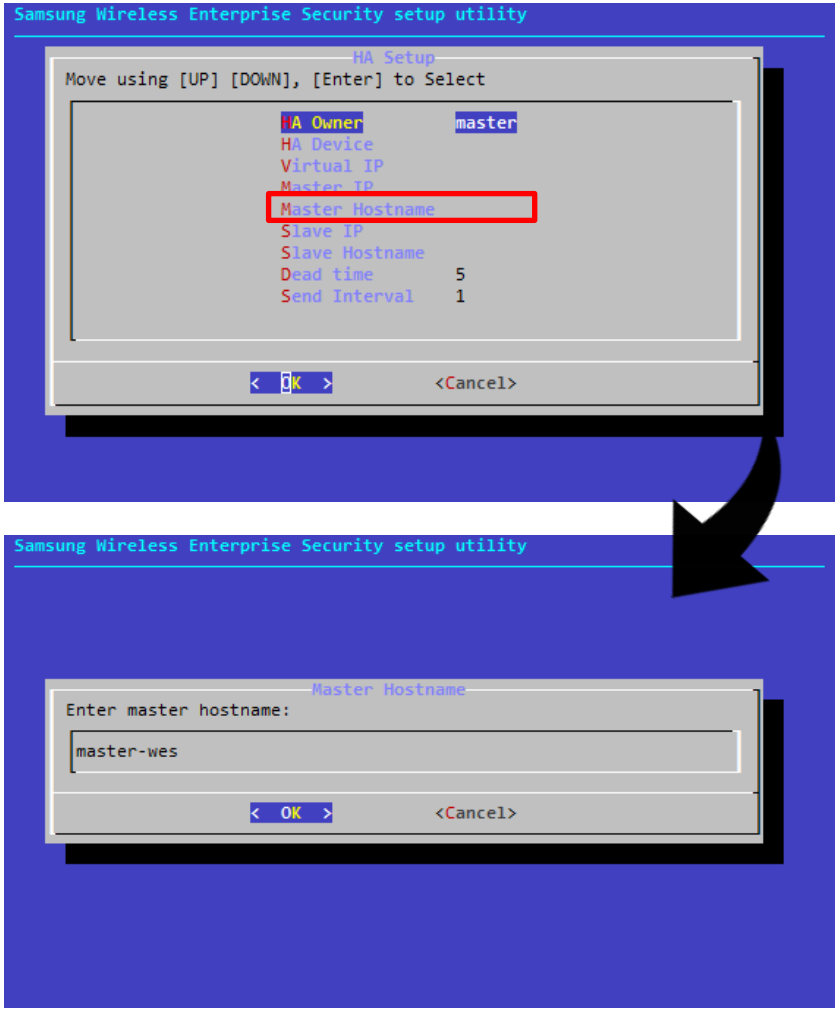
2.1.2 High Availability Servers

How to configure servers for High Availability Mode:

- **Perform these setup steps on both servers.**

- **Select ‘Master Hostname’.**

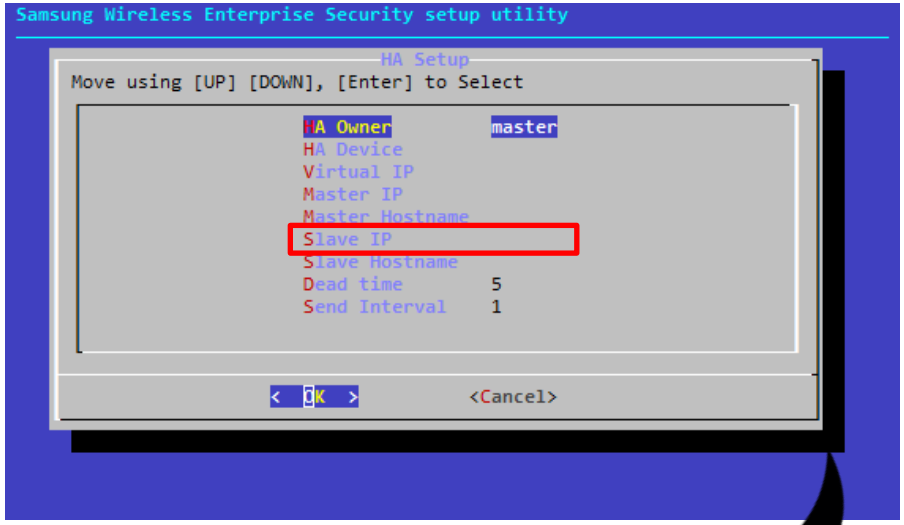
- **Enter the hostname of the Master (Active) server**



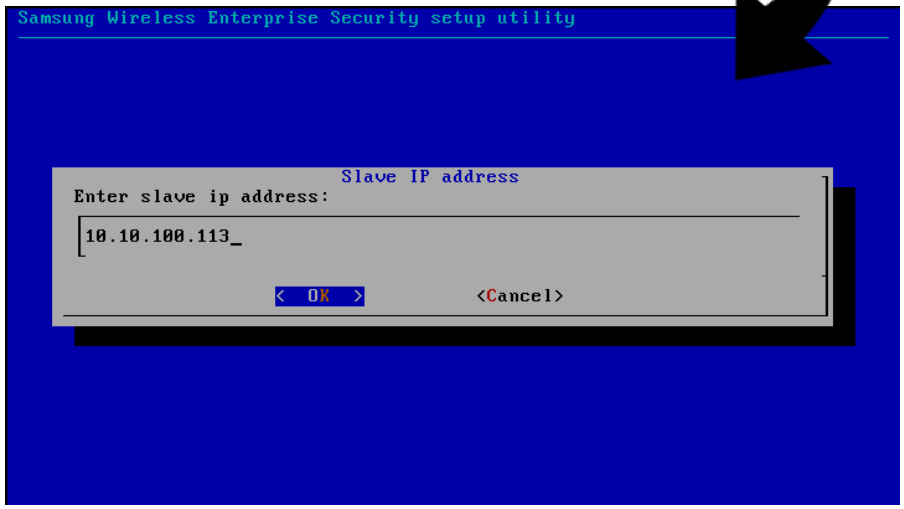
2.1.2 High Availability Servers

How to configure servers for High Availability Mode:

- **Perform these setup steps on both servers.**



- **Select ‘Slave IP’.**



- **Enter IP address of the Slave (Standby) server**

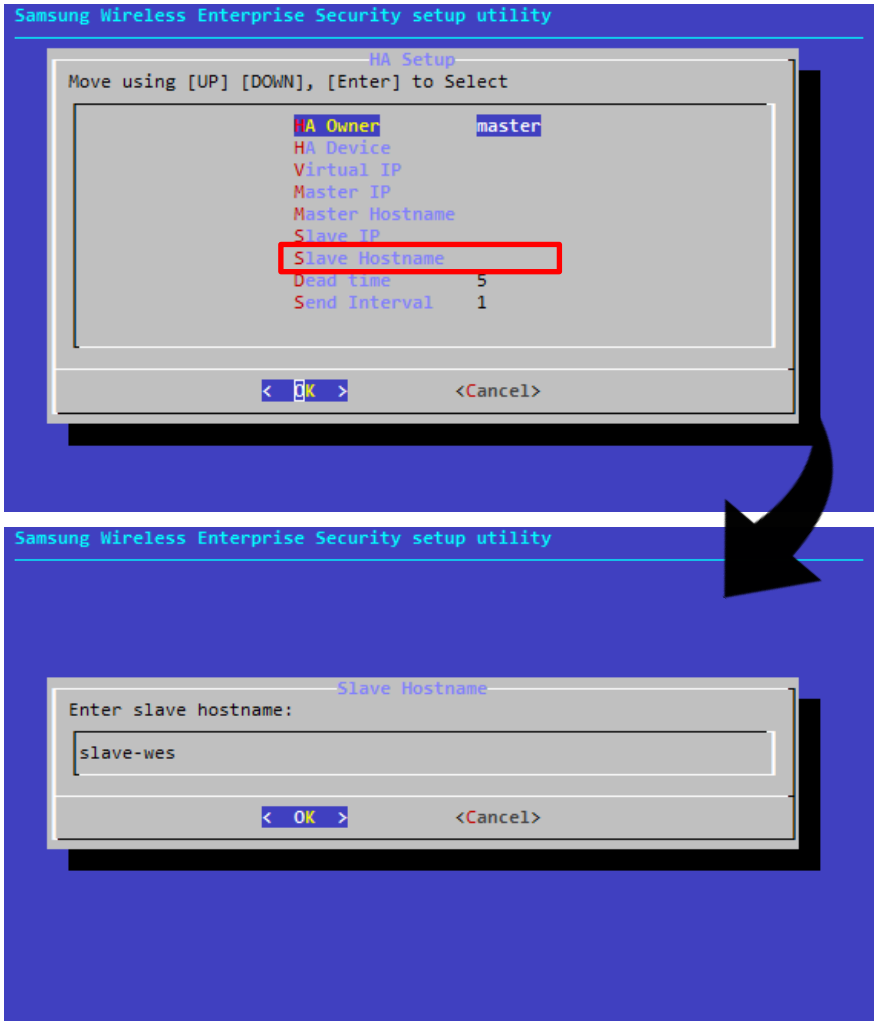
2.1.2 High Availability Servers

How to configure servers for High Availability Mode:

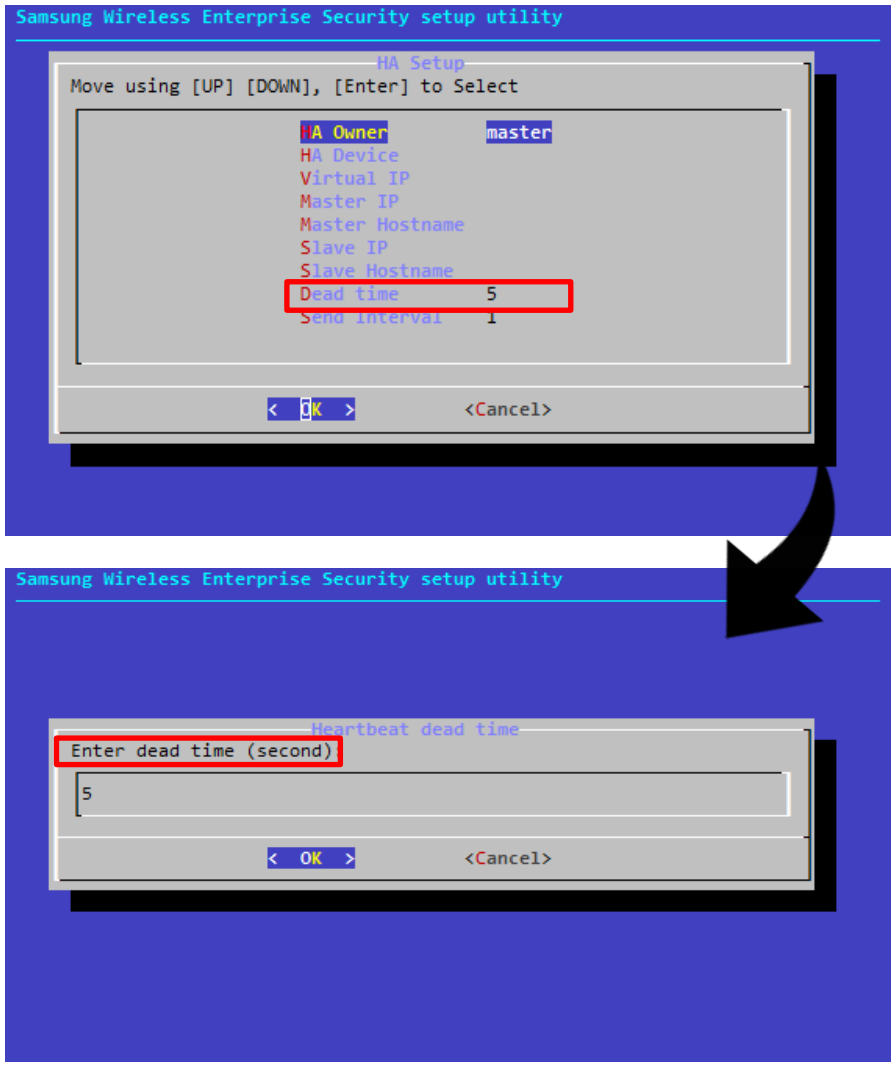
- **Perform these setup steps on both servers.**

- **Select ‘Slave Hostname’.**

- **Enter the hostname of the Slave (Standby) server**



2.1.2 High Availability Servers



How to configure servers for High Availability Mode:

- **Perform these setup steps on both servers.**

- **Select 'Dead Time'.**

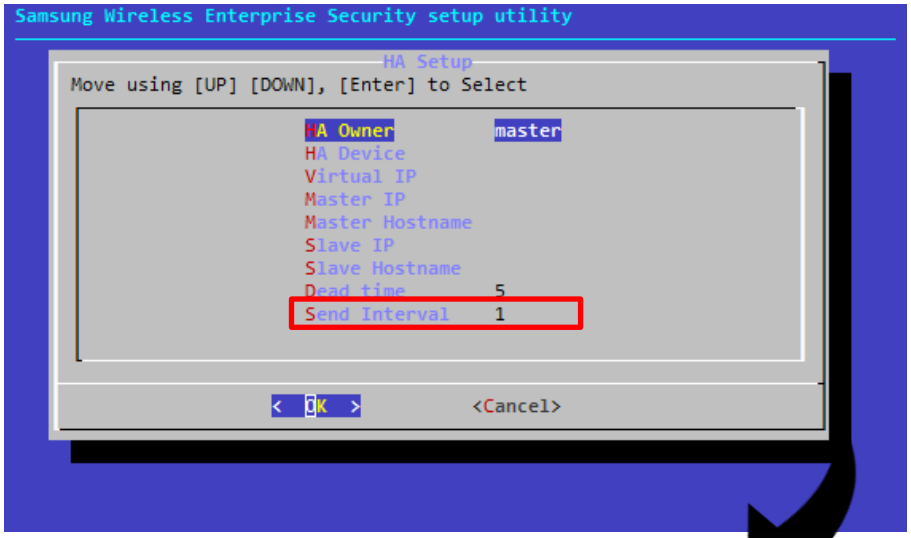
- **Enter the response wait time in seconds.**
- **This value is the amount of time that the server will wait for a health check (heartbeat) message from the other server. If it does not see the message from the other server then a failover is triggered.**
- **This value must be larger than the Send Interval**

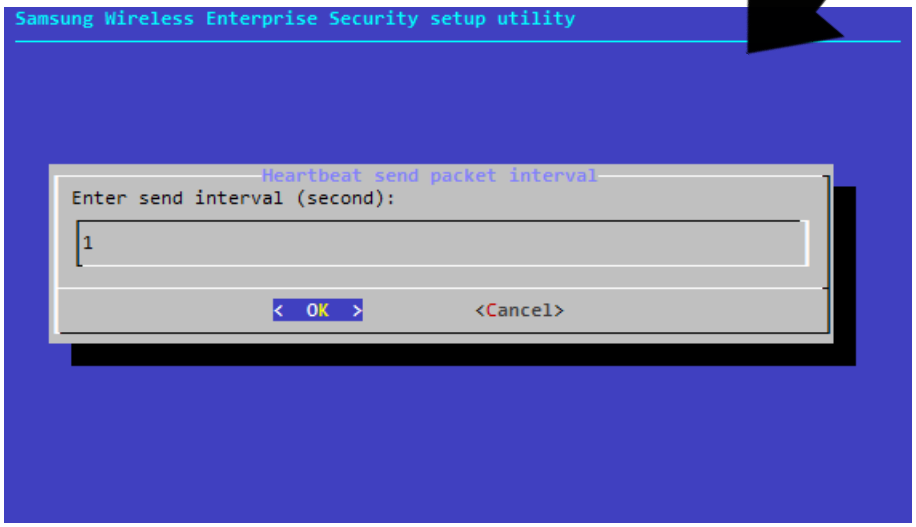
2.1.2 High Availability Servers

How to configure servers for High Availability Mode:

- **Perform these setup steps on both servers.**

- **Select ‘Send Interval’.**



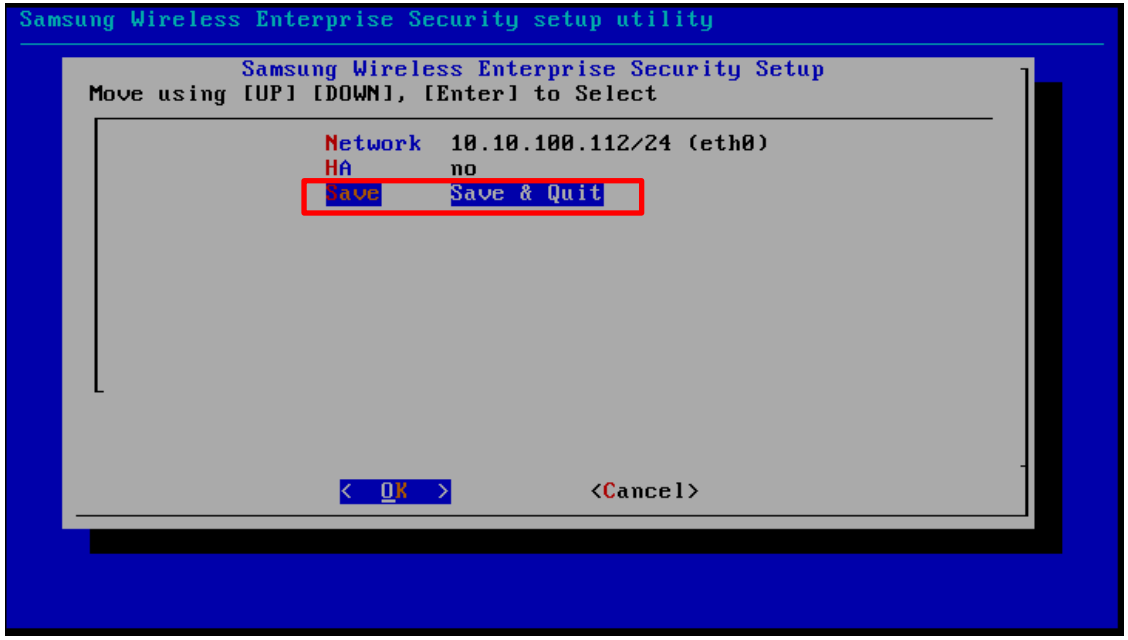


- **Set the health check message transmission cycle time in seconds.**
- **This value must be smaller than the Dead Time value.**

2.1.2 High Availability Servers

How to configure servers for High Availability Mode:

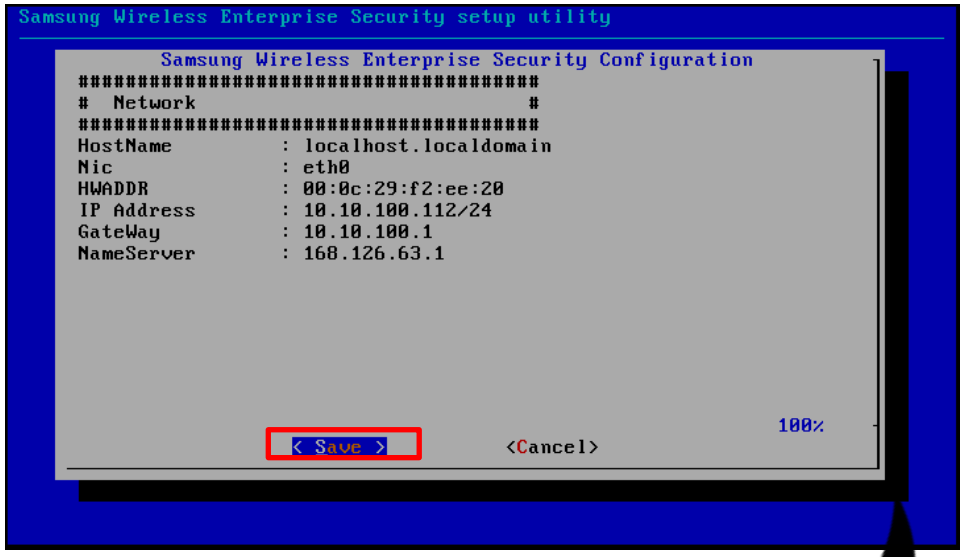
- **Perform these setup steps on both servers.**



- To apply settings, select 'Save & Quit’

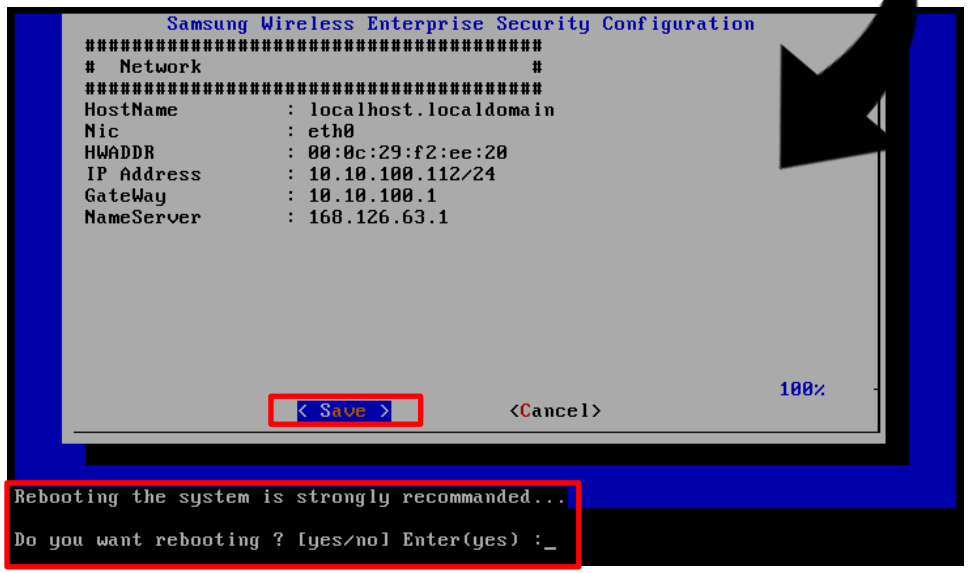
2.1.2 High Availability Servers

Verify the settings entered and select ‘Save’



Type ‘Yes’ to reboot the server in order to complete the configuration.

Your server will reboot into the normal WES operating mode.



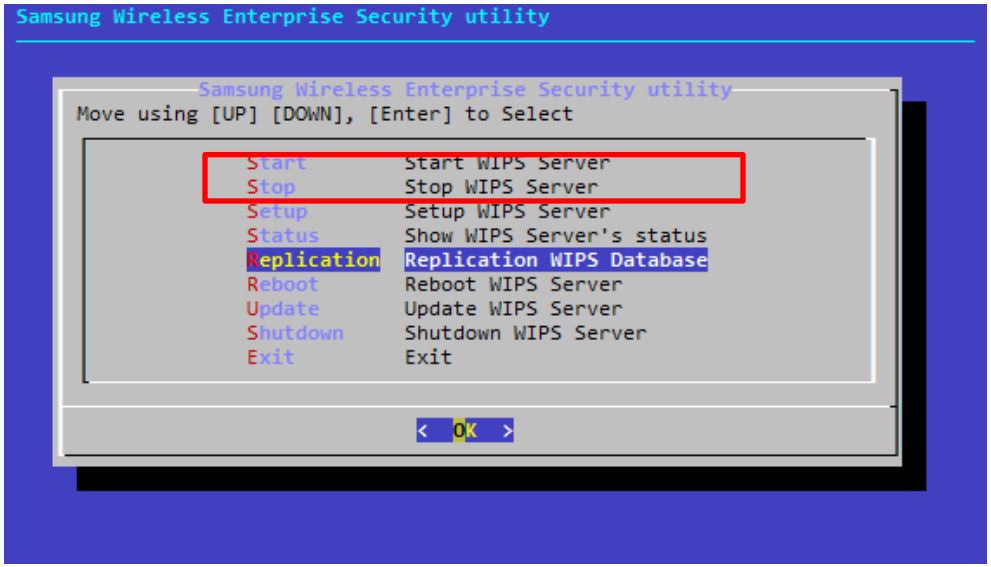
2.1.2 High Availability Servers

How to configure servers for High Availability Mode:

- **This step should only be performed on the Master (Active) Server.**
- **Perform this step ONLY after finishing the setup steps on the Slave (Standby) server.**

- **Select 'Replication'.**
- **This step synchronizes the databases between your Master (Active) and Slave (Standby) Servers.**
- **When prompted for a password, enter: adminme09@**

- **When this step is complete, your WES servers will be running in normal High Availability mode.**

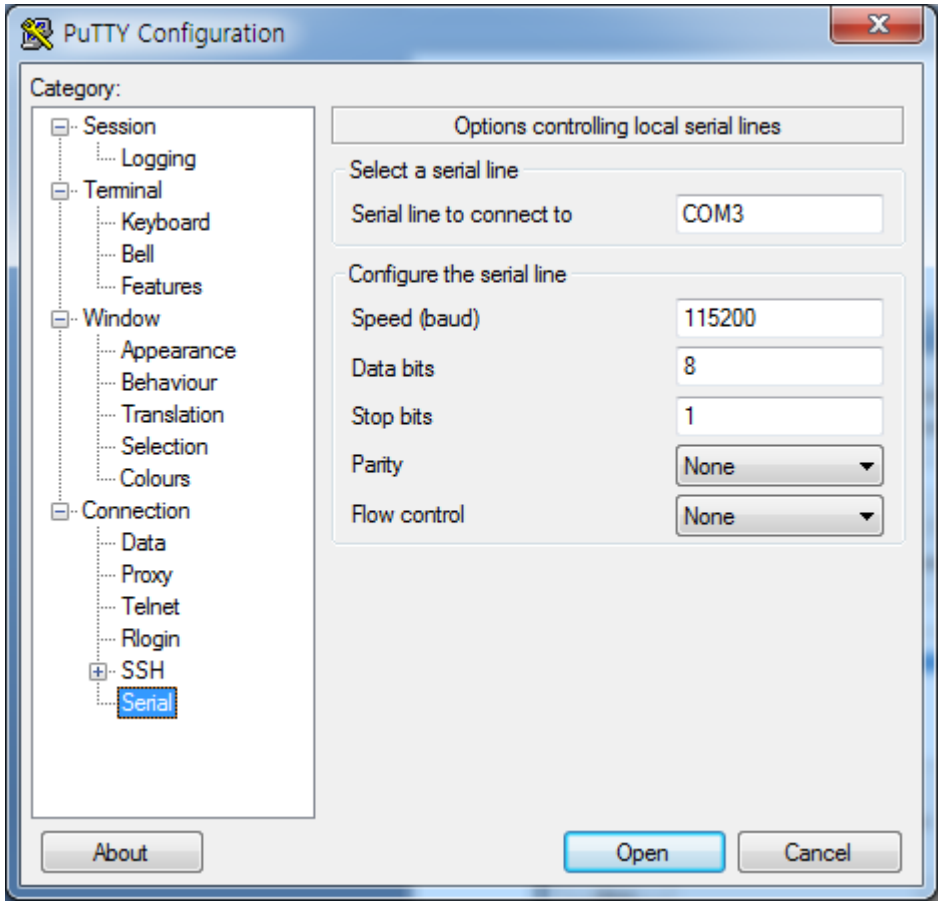


2.2 Sensors

2.2 Sensors

- **This section details how to manually configure your AP using the console to run in Sensor mode.**

- Please use a station emulator like a PuTTY to program the AP
- Use the following connection values:
- Speed : 115200
- Data bits : 8
- Stop bits : 1
- Parity : None
- Flow control : None



※ Connect SSH(telnet) Sensor : SSH port : 50022, telnet port : 50023

- Enter ID and Password for your AP to login

```
 WEA302i ppc #2 Tue Sep 16 10:04:17 KST 2014 (none)
Login:
 WEA302i ppc #2 Tue Sep 16 10:04:17 KST 2014 (none)
Login: root
Password:
SAMSUNG ELECTRONICS CO., LTD. Login
234_30x# config interface address
      Usage: 234_30x/address <IPADDR> <NETMASK> <GATEWAY>
234_30x# show config wips summary
wips mode ..................................... WIPS_AP_SENSOR_MODE
wips server ip ................................ 10.10.100.112
wips nat ...................................... 1
wips sharedkey ................................ jtkim
234_30x#
```

- The current operating mode of the sensor can be viewed by typing

  "`show config wips summary`"

- To change the operating mode from AP to Sensor, type "`config wips mode <sensor>`"
  - Note: The AP will reboot after this command is entered.
- Sensor + Integrated AP type can be set through the GUI if employing an APC Link

```
234_30x# show config interface summary
Name ..................................... br0
Mode ..................................... Static
MAC ...................................... F4:D9:FB:35:7F:AD
IP address ............................... 10.10.100.125
Subnet Mask .............................. 255.255.255.0
Gateway address .......................... 10.10.100.1
PHY Status ............................... UP
Interface Status ......................... UP
234_30x#
234_30x#
234_30x#
234_30x#
234_30x# config interface address
      Usage: 234_30x/address <IPADDR> <NETMASK> <GATEWAY>
234_30x# config interface address 10.10.100.117 255.255.255.0 10.10.100.1
234_30x#
```

- You can check the network setting information of the sensor by typing

  "`show configure interface summary`"

- To change the sensor's network settings, type

  "`config interface address <IPADDR> <NETMASK> <GATEWAY>`"

```
212_30x# show config wips summary
wips mode ..................................... WIPS_SENSOR_MODE
wips server ip ................................ 10.10.200.162
wips nat ...................................... 1
wips sharedkey ................................ 00000000
```

- Sensor server link info can be viewed (server IP, NAT mode, shared key) by entering “show config wips summary”

```
212_30x# config wips server
     Usage: 212_30x/server <wips_serverip><wips_nat><shared_key>
212_30x# config wips server 0.0.0.0 1 00000000
```

- To modify server link settings type ““config wips server <wips server ip> <nat mode> < shared key >”
  - To not use NAT mode(X) = 1, Use NAT mode(O) =2
  - If not using NAT mode : connected from server to sensor
  - If using NAT mode : connected from sensor to server

```
212_30x# show config wips summary
wips mode ..................................... WIPS_SENSOR_MODE
wips server ip ................................ 10.10.100.112
wips nat ...................................... 2
wips sharedkey ................................ 00000000
```

Samsung Wireless Enterprise

2.3 Network Ports

2.3 Network Ports

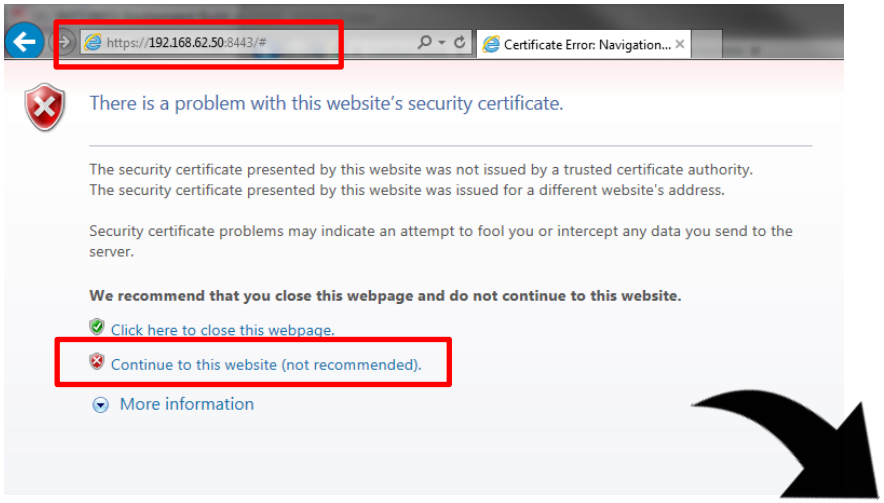
Port number	Listen	Purpose	Remarks
13444/TCP	Server Listen	Sensor-Server communication Sensor Upgrade	Sensor < -> Server
22/TCP	Server Listen	Connection Server Cli (SSH)	Manager -> Server
50022/TCP	Sensor Listen	Connection Sensor Cli(SSH)	Manager -> Sensor
50023/TCP	Sensor Listen	Connection Sensor Cli(Telnet)	Manager -> Sensor
8443/TCP	Server Listen	Connection Server GUI	Manager -> Server
161/UDP	APC Listen	APC Link(SNMP)	
2002/TCP	Server Listen	Troubleshooting Sensors	Sensor -> Manager
22/TCP	Server Listen	APC data Link	APC -> Server

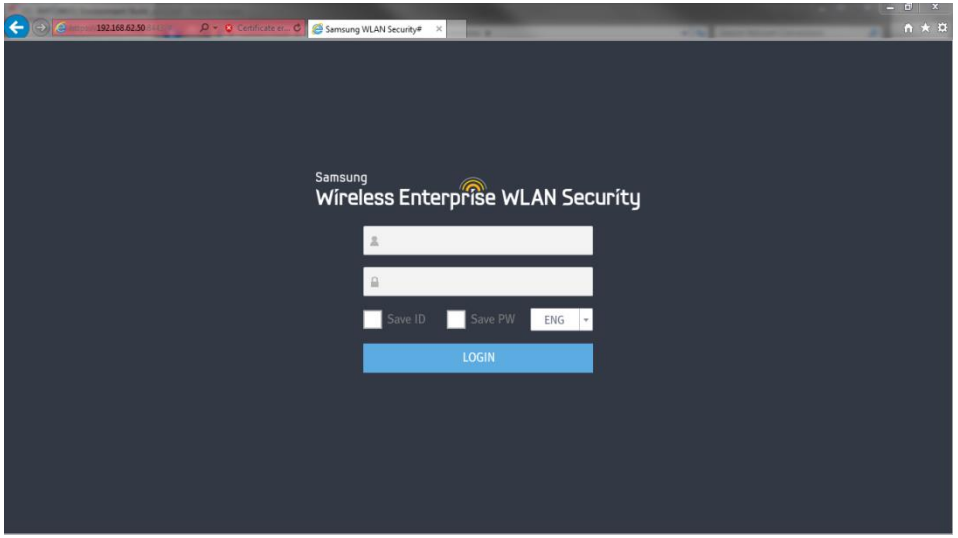
Samsung Wireless Enterprise

2.4 Administrator GUI

2.4 Administrator GUI

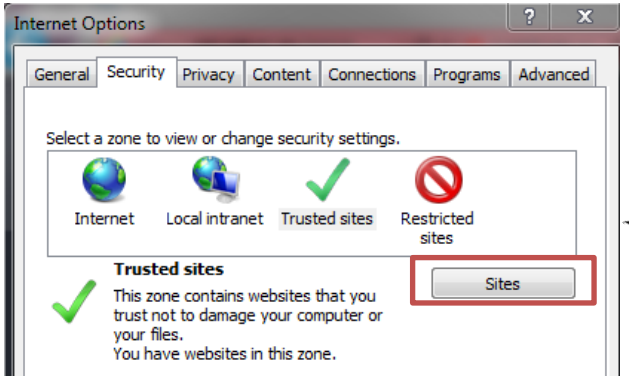
- Access the web browser based administrator GUI by connecting to:
  - https://<WES Virtual IP address>:8443

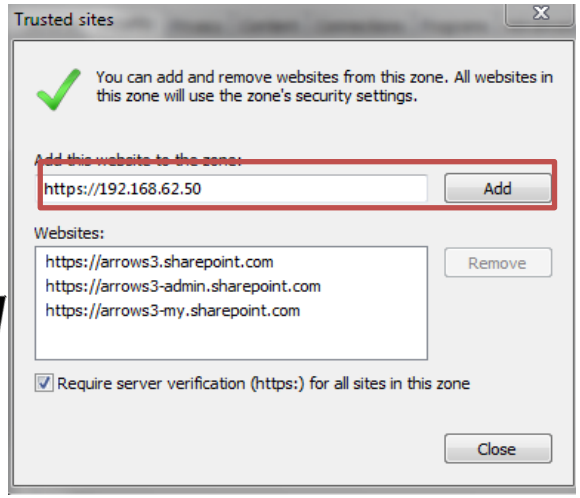




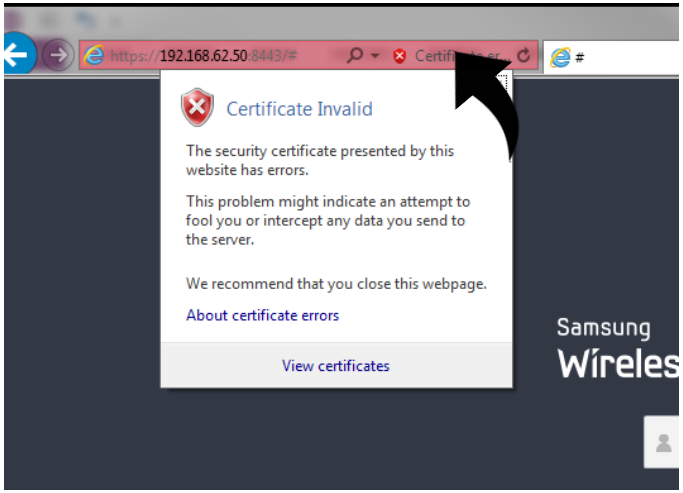
- Select the “Continue to this website” option.
  - The WES security certificate will have to be manually installed to bypass this warning screen.

- How to manually install the website certificate:
  - In Internet Options > Security > Trusted Sites, add the WES GUI address to the list of trusted sites.

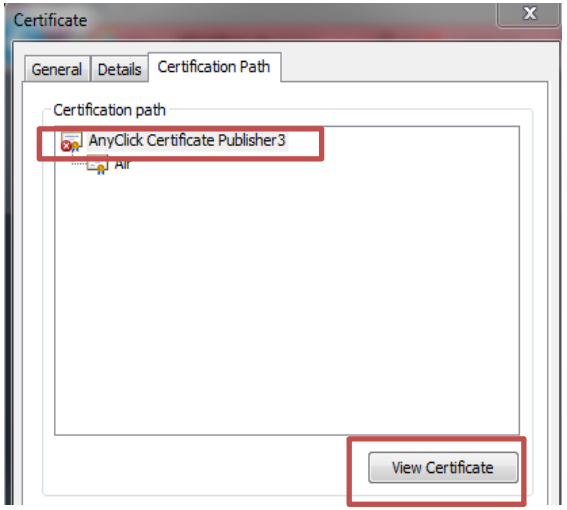




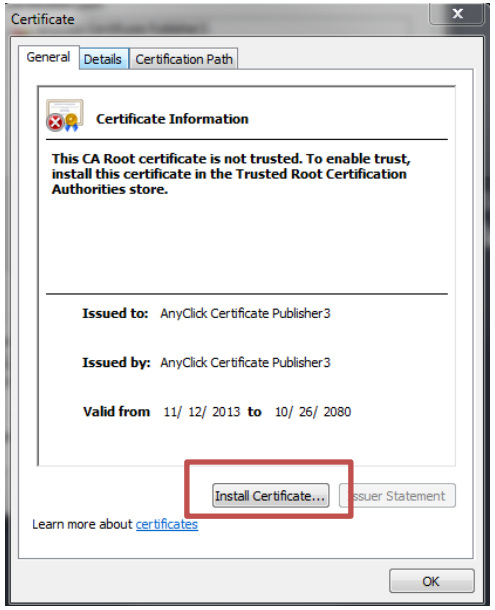
- Click on the Certificate Error Warning in the Browser Address bar, then select “View Certificates”



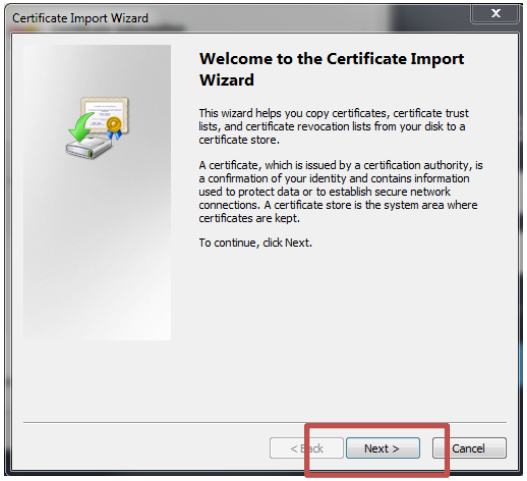
- In the Certificate Window, go to the “Certification Path” tab.
- Select the “AnyClick Certificate Publisher 3”
- Click on “View Certificate”



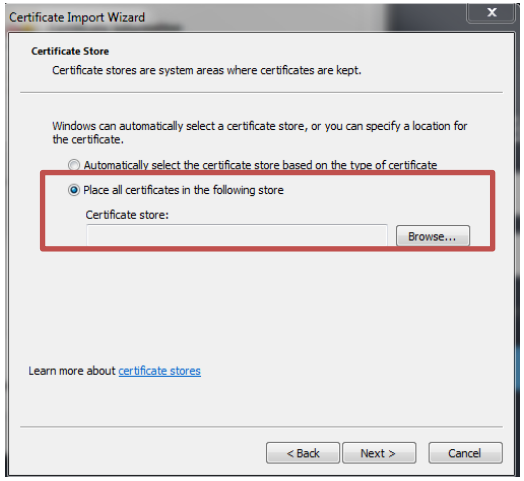
- Click on “Install Certificate”



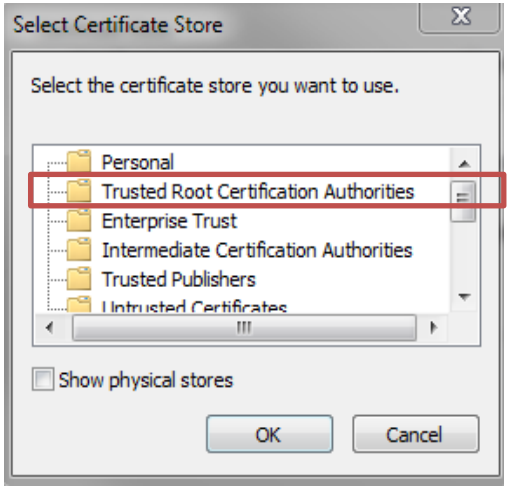
- On the Wizard, click “Next”



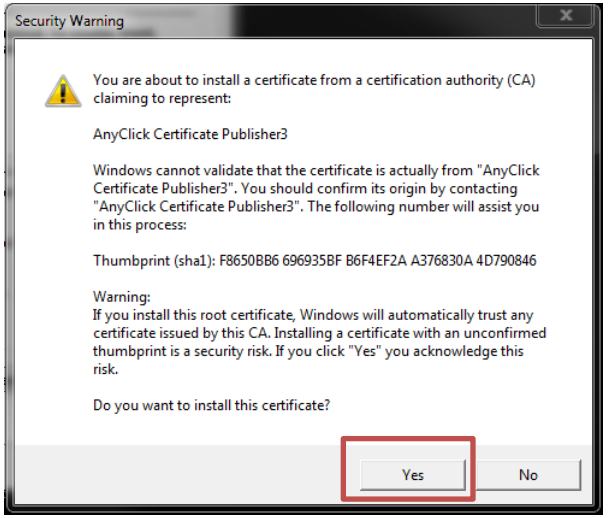
- Select “Place all certificates in the following store”
- Click on “Browse



- Select “Trusted Root Certification Authorities”
- Click “OK”



- Click “Next” and “Finish” on the remaining wizard screens.

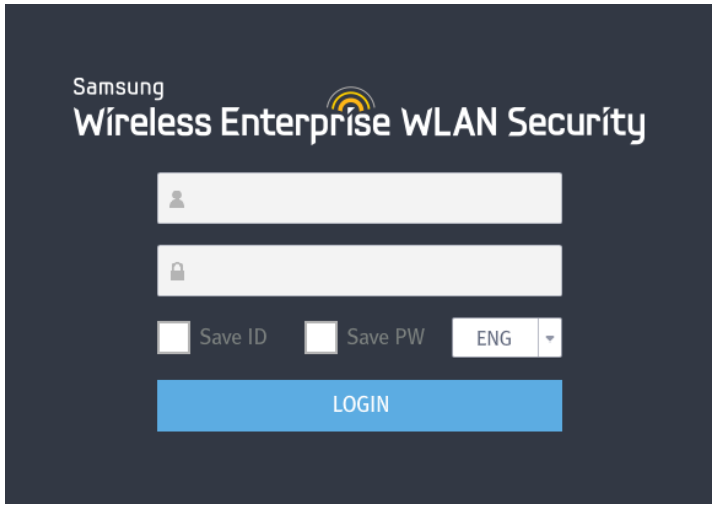


- You will receive the following warning, click on “Yes”.

- Close the remaining Certificate windows.
- Now when browsing to the GUI address, the certificate warning screen is bypassed.

2.4 Administrator GUI

- Use the following credentials to login to the administrator for the first time:
- User ID: samsung
- Password: samsung00!



- An initial configuration dialog box will appear.
- Here you create the Root Administrator Account.
- After creating the root admin account, you may login with that account.