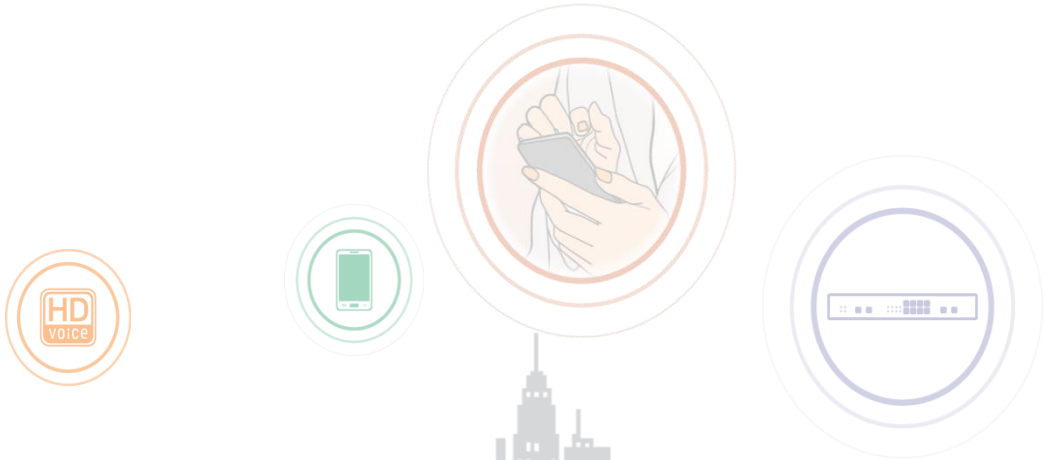
Samsung Wireless Enterprise™

Samsung WLAN

Day 2



Day 2 Outline

Samsung Wireless Enterprise™

1. Lab Exercise
   - 1.1 Complete Rebuild

2. APC and AP Troubleshooting
   - 2.1 System Logs
   - 2.2 Station Tracking
   - 2.3 Packet Capture
   - 2.4 Tech Support

3. Advanced Deployment
   - 3.1 Remote AP
   - 3.2 Internal Radius Server
   - 3.4 Quality of Service
   - 3.5 VQM
   - 3.6 Root and Repeater AP
   - 3.7 SNMP

4. Security
   - 4.1 Firewall / ACL
   - 4.2 Captive Portal
   - 4.3 Web Passthrough
   - 4.4 Conditional Web Redirection

Samsung Wireless Enterprise™

1. Lab Exercise

- 1.1 Complete Rebuild

Use the WLAN_day2morning_LAB to complete

Please complete this lab by 12:00pm.

The instructor is here to help

Samsung Wireless Enterprise™

2. APC and AP Troubleshooting

- 2.1 System Logs
- 2.2 Station Tracking
- 2.4 Tech Support
- 2.5 Interference Devices
- 2.6 Rogue AP's and Stations

2.1 System Logs

Alarm/Event

Debug log/detailed log

2.1 System Logs

Samsung Wireless Enterprise™

ALARM

```
WEC8500# show alarm info
1 system      MAJ Software Down
2 system      MAJ Cpu Load Alarm
3 system      MAJ Memory Usage Alarm
4 system      MAJ Disk Usage Alarm
5 system      MAJ Fan Rpm Alarm
6 system      CRT System Temperature Alarm
7 system      CRT System Thermal Runaway
8 system      MAJ DHCP Sever Connect Failure
9 system      MAJ DNS Server Connect Failure
10 system      MAJ NTP Server Connect Failure
11 system      CRT Fan Fail alarm
12 system      CRT Temperature Sensor Fail
13 system      MAJ Power Module Fail
14 ap          CRT Duplicated IP
15 ap          CRT No Radio
16 ap          CRT License Expired
17 ap          MAJ BSS INTERFACE DN
18 ap          MAJ AP
19 ap          MAJ AP CPU Load High
20 ap          MAJ AP MEM Usage High
21 ap          MAJ AP Monitor Device Fail
22 ap          MAJ AP RADIO CARD TX FAIL
23 ap          MIN AP CHANNEL BUSY
24 ap          MAJ AP DISK USAGE HIGH
25 wifi        MIN CAC Minor Calls
26 wifi        MAJ CAC Major Calls
27 wifi        MAJ CLUSTER APC Lost Connection
28 security    CRT Radius Servers Failed
29 network     MAJ NET Link dn
30 se          MIN SE VQM Excess Burst
31 se          MIN SE VQM Excess Delay
32 se          MIN SE VQM Low MOS
33 se          CRT SE NFM SE_RESTART
```

```
WEC8500# show alarm conf
-----------------------------------------
        Alarm Log Configuration
-----------------------------------------
 Alarm Group Filter          all
 Alarm Level Filter          minor
 Alarm Log File Size         10 MBytes
 Alarm Log File Count        2
 Alarm Log STD Out           Off
```

```
WEC8500# show alarm list all
1 system      2013-04-02 10:54:34 MAJ APC  Power Module Fail POWER0
2 network     2013-04-02 10:54:31 MAJ APC ge6 NET Link dn
AdminStatus[up] OperStatus[down]
3 network     2013-04-02 10:54:31 MAJ APC ge5 NET Link dn
AdminStatus[up] OperStatus[down]
4 network     2013-04-02 10:54:31 MAJ APC ge7 NET Link dn
AdminStatus[up] OperStatus[down]
5 network     2013-04-02 10:54:31 MAJ APC xe2 NET Link dn
AdminStatus[up] OperStatus[down]
6 network     2013-04-02 10:54:31 MAJ APC ge8 NET Link dn
AdminStatus[up] OperStatus[down]
7 network     2013-04-02 10:54:31 MAJ APC xe1 NET Link dn
AdminStatus[up] OperStatus[down]
8 network     2013-04-02 10:54:29 MAJ APC mgmt0 NET Link dn
AdminStatus[up] OperStatus[down]
```

```
WEC8500# show alarm list ?

      all             Display the list of active alarms
      group           Display the list of active alarms for
                      specific group
      level           Display the list of active alarms for
                      specific level
```

2.1 System Logs

Samsung Wireless Enterprise™

 # Alarm Log Size(Default : 10MBytes) is occupied by event messages

 # Event messages include Alarm messages

Alarm Configuration

```
WEC8500/configure# alarm ?

      backupIP                  Configure backup AP controller IP address
      current-terminal          Configure logging alarms on/off for a current terminal
      dump                      Convert alarm log DB to dump txt file
      group                     Configure alarm for specific group
      level                     Configure alarm for specific level
      logcount                  Configure the number of backup file for alarm log (Default : 2)
      logsize                   Configure file size for alarm log
      stdout                    Configure standard out on/off for all terminals
```

```
WEC8500# show alarm history all
1 network    2013-04-04 18:41:10 MAJ APC ge4 NET Link dn Clear AdminStatus[up] OperStatus[up]
2 network    2013-04-04 18:41:06 MAJ APC ge4 NET Link dn Declare AdminStatus[up] OperStatus[down]
3 network    2013-04-04 18:40:49 MAJ APC ge1 NET Link dn Clear AdminStatus[up] OperStatus[up]
4 network    2013-04-04 18:40:43 MAJ APC ge1 NET Link dn Declare AdminStatus[up] OperStatus[down]
5 network    2013-04-04 18:40:29 MAJ APC ge1 NET Link dn Clear AdminStatus[up] OperStatus[up]
6 network    2013-04-04 18:40:16 MAJ APC ge1 NET Link dn Declare AdminStatus[up] OperStatus[down]
7 network    2013-04-04 11:35:05 MAJ APC vlan1.2202 NET Link dn Clear AdminStatus[up] OperStatus[up]
8 network    2013-04-04 11:34:11 MAJ APC vlan1.2201 NET Link dn Clear AdminStatus[up] OperStatus[up]
9 network    2013-04-02 10:54:43 MAJ APC vlan1.1 NET Link dn Clear AdminStatus[up] OperStatus[up]
```

Show Event

```
WEC8500# show event
1 network     11:26:13 NOT APC IP Duplication detect IP:1.111.60.63 MAC:94:63:d1:a5:34:63 Interface:vlan1.1217
2 network     11:26:12 NOT APC IP Duplication detect IP:1.111.60.63 MAC:94:63:d1:a5:34:63 Interface:vlan1.1217
3 wifi        11:24:36 NOT  RRM DPC RUN Dynamic power control done [2.4GHz]
4 wifi        11:24:35 NOT  RRM DPC RUN Dynamic power control done [5GHz]
5 network     11:21:02 NOT APC IP Duplication detect IP:1.110.19.18 MAC:0c:df:a4:2b:6f:97 Interface:vlan1.1212
6 network     11:21:01 NOT APC IP Duplication detect IP:1.110.19.18 MAC:0c:df:a4:2b:6f:97 Interface:vlan1.1212
7 network     11:19:59 NOT APC IP Duplication detect IP:1.111.195.49 MAC:0c:df:a4:2c:7f:67 Interface:vlan1.1202
8 network     11:19:58 NOT APC IP Duplication detect IP:1.111.195.49 MAC:0c:df:a4:2c:7f:67 Interface:vlan1.1202
9 wifi        11:14:37 NOT  RRM DPC RUN Dynamic power control done [2.4GHz]
10 wifi        11:14:35 NOT  RRM DPC RUN Dynamic power control done [5GHz]
```

2.1 System Logs

Samsung Wireless Enterprise™

Debug Log / Log Detail

```
WEC8500# show debug processes
Processes Debug Info.

id          name       pid       runmode argument
--        ------    ------        ------ ------
 0       swmmon      1719     exec-ever
 1           db      1720     exec-ever
 2          evm      1746     exec-ever
 3      evmlogd      1747     exec-ever
 4      license      1748     exec-ever
 5         pcap      1749     exec-ever
                     .
                     .
                     .
26      hostapd      2458     exec-ever
27         wids      2459     exec-ever
28 guestService      2460     exec-ever
29          eqm      2461     exec-ever
30          vqm      2462     exec-ever
31         irfm      2463     exec-ever
32        rfsgw      2546     exec-ever
33        apclt      2581     exec-ever
34           pm      2582     exec-ever
35       sipalg      2585     exec-ever
36       httprd      2591     exec-ever
37        snmpd      2625     exec-ever -z
/tmp/SNMP/OIDInfoDataFile.CPS
38     WebAgent      2626     exec-ever -z
/tmp/SNMP/OIDInfoDataFile.CPS
39         salh      2627     exec-ever
40      ipwlogd      2628     exec-ever
41          nfm      2629     exec-ever
42         cron      1533 monitor-only
43      syslogd      1521 monitor-only
44        klogd      1525 monitor-only
45           ui      2696     exec-ever
```

```
WEC8500# show debug log conf
-------------------------------------------
        Debug Log Configuration
-------------------------------------------
 Debug Log Mode                  On
 Debug Log Module Filter         all
 Debug Log Level Filter          warning
 Debug Log File Size             10 MBytes
 Debug Log File Count            2
 Module STD Out                  Off
 Module Filter STD Out           all
 Module Level Filter STD Out     debug
```

```
WEC8500# show debug log detail conf
-----------------------------------------------
        Debug Detail Log Configuration
-----------------------------------------------
 Debug Detail Log Mode              On
 Debug Detail Log Module Filter     all
 Debug Detail Log Level Filter      information
 Debug Detail Log File Size         100 MBytes
 Debug Detail Log File Count        2
 Debug Detail Log STD Out           Off
```

```
WEC8500# debug log ?

      detail    Log debug in detail
      dump      Convert legacy DB debug file to txt file
      level     Configure debug message for specific level
      logcount  Configure the number of backup file for debug log
      logsize   Configure file size for debug log
      module    Configure debug message for specific module
      mstdout   Configure the module Standard Out on/off for debug message
      off       Configure debug log off
      on        Configure debug log on
```

2.1 System Logs

```
npi_wec8500# configure terminal
npi_wec8500/configure# alarm stdout on
 Alarm Log STDOUT On
npi_wec8500/configure# *2013-11-21 13:05:59 #wifi-NOT: RRM DCS RUN APC Notice
[Normal Run] Dynamic channel selection done [5GHz]
*2013-11-21 13:07:00 #wifi-NOT: RRM DCS RUN APC Notice [Normal Run] Dynamic channel
selection done [2.4GHz]
*2013-11-21 13:07:59 #wifi-NOT: RRM DCS RUN APC Notice [Normal Run] Dynamic channel
selection done [5GHz]

npi_wec8500/configure# alarm stdout off
 Alarm Log STDOUT Off
npi_wec8500/configure#
```

Samsung Wireless Enterprise™

Lab 16 -

Telnet into the APC and look at System logs

1. Telnet to the APC “192.168.xx.10”
2. Practice with these show commands “Alarms” WEA8500#
    1. show alarm info
    2. show alarm conf
    3. show alarm list all
    4. show alarm list ?
    5. show alarm history all
    6. show event
3. Go to configure mode → WEA8500# configure terminal
4. WEA8500/configure# alarm ?
5. Type exit
6. Practice with these commands “Debugs” from WEA8500#
    1. show debug processes
    2. show debug log conf
    3. show debug log detail conf
    4. debug log ?

2.2 Station Tracking

Samsung Wireless Enterprise™

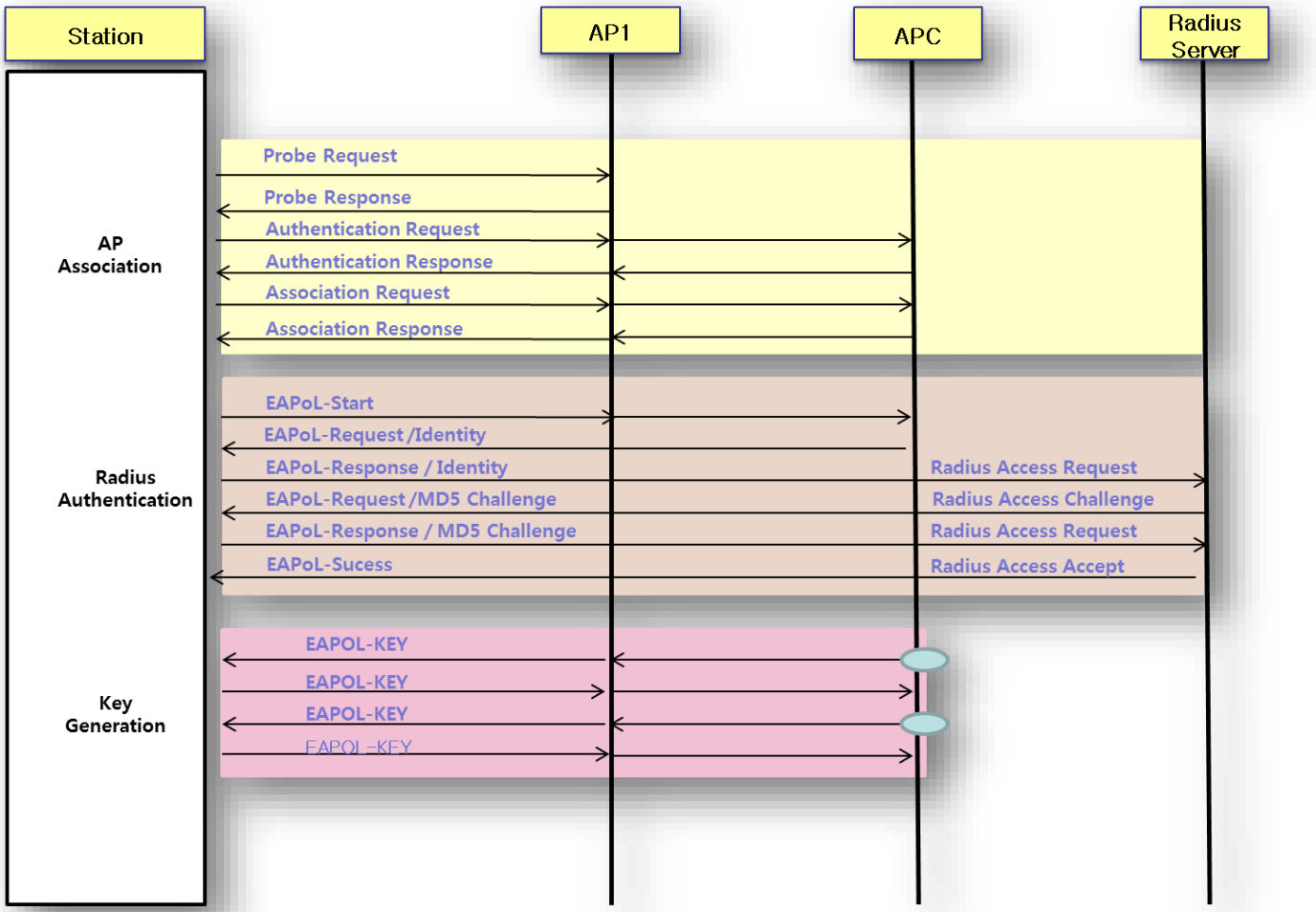
2.2.1 Station Tracking History

2.2.2 Station Tracking Real-time

2.2.1 Station Tracking History

Samsung Wireless Enterprise™

The Flow of Authentication of WLAN Station



2.2.1 Station Tracking History

Samsung Wireless Enterprise™

Trace the Station - Association

```
WEC8500# show stationtracking station 38:AA:3C:3D:B7:20
38 TR_38AA3C3DB720 [2013-04-08:10:35:43.524] INF <dr_vlan1_1217> Forwarded BOOTREPLY[DHCPACK] for 38:aa:3c:3d:b7:20 to 10.65.182.216
39 TR_38AA3C3DB720 [:10:35:43.523] INF <dsub_dhcpr> DHCP PLD: 38:aa:3c:3d:b7:20 station ip set 10.65.182.216
40 TR_38AA3C3DB720 [:10:35:43.523] INF <dr_vlan1_1217>   [DHCPACK] received from dhcp server
41 TR_38AA3C3DB720 [:10:35:43.521] INF <dr_vlan1_1217> Forwarded BOOTREQUEST[DHCPREQUEST] for 38:aa:3c:3d:b7:20 to 10.64.2.31
42 TR_38AA3C3DB720 [:10:35:43.520] INF <dr_vlan1_1217>   [DHCPREQUEST] received from dhcp client
43 TR_38AA3C3DB720 [:10:35:43.515] INF <dr_vlan1_1217> Forwarded BOOTREPLY[DHCPOFFER] for 38:aa:3c:3d:b7:20 to 10.65.182.216
44 TR_38AA3C3DB720 [:10:35:43.515] INF <dr_vlan1_1217>   [DHCPOFFER] received from dhcp server
45 TR_38AA3C3DB720 [:10:35:43.514] INF <dr_vlan1_1217> Forwarded BOOTREQUEST[DHCPDISCOVER] for 38:aa:3c:3d:b7:20
46 TR_38AA3C3DB720 [:10:35:43.513] INF <dr_vlan1_1217>   [DHCPDISCOVER] received from dhcp client
47 TR_38AA3C3DB720 [:10:35:43.246] INF <security> STA(38:aa:3c:3d:b7:20) - PMKSA-Add: apc=1 pmkid[89,77,9c,..,88,b3,cb]
48 TR_38AA3C3DB720 [:10:35:43.244] INF <security> STA(38:aa:3c:3d:b7:20) - Authenticated. user=nwtest51 vlan=1217 qos=0 acl=setup url=<none>
49 TR_38AA3C3DB720 [:10:35:43.244] INF <security> STA(38:aa:3c:3d:b7:20) - SetFlag[Auth]: wlan=1 802.1x=1 dynVlan=1 aaa=1 vlan=1217 qos=0
ap=61 radio=1
50 TR_38AA3C3DB720 [:10:35:43.244] INF <security> STA(38:aa:3c:3d:b7:20) - CAPWAP Send: SetSessionKey: seq=0x00000000 wlan=1 ap=61 radio=1
51 TR_38AA3C3DB720 [:10:35:43.243] INF <security> STA(38:aa:3c:3d:b7:20) - EAPOL-Key: Recv 4/4 msg of 4-way h/s
52 TR_38AA3C3DB720 [:10:35:43.241] INF <security> STA(38:aa:3c:3d:b7:20) - EAPOL-Key: Send 3/4 msg of 4-way h/s
53 TR_38AA3C3DB720 [:10:35:43.241] INF <security> STA(38:aa:3c:3d:b7:20) - EAPOL-Key: Recv 2/4 msg of 4-way h/s
54 TR_38AA3C3DB720 [:10:35:43.224] INF <security> STA(38:aa:3c:3d:b7:20) - EAPOL-Key: Send 1/4 msg of 4-way h/s
55 TR_38AA3C3DB720 [:10:35:43.224] INF <security> STA(38:aa:3c:3d:b7:20) - RADIUS Recv[Auth]: ACCESS-ACCEPT msg. id=0x12 len=399
56 TR_38AA3C3DB720 [:10:35:42.930] INF <security> STA(38:aa:3c:3d:b7:20) - 802.1x Auth Started. reassoc
57 TR_38AA3C3DB720 [:10:35:42.930] INF <security> STA(38:aa:3c:3d:b7:20) - Authentication started
58 TR_38AA3C3DB720 [:10:35:42.929] INF <security> STA(38:aa:3c:3d:b7:20) - PMK not found for OKC
59 TR_38 curity> STA(38:aa:3c:3d:b7:20) - (Re)Assoc: PMKID[0][c8,2a,ee,..,9
60 TR_38 curity> STA(38:aa:3c:3d:b7:20) - (Re)Assoc: 1 PMKIDs Received
61 TR_38 curity> STA(38:aa:3c:3d:b7:20) - New STA-Info: Added. wlan=1 ap=61 radio=1 count=2
62 TR_38AA3C3DB720 [:10:35:42.928] I <security> STA(38:aa:3c:3d:b7:20) - STA PLD: Created. wlan=1 ap=61 radio=1 id=172
63 TR_38AA3C3DB720 [:10:35:42.925] INF [I:STA] Association - BSSID(f4:d9:fb:35:6c:c2) STA(38:aa:3c:3d:b7:20)
```

STA IP

Attributes received from Authentication Server

Authentication Completed

Process of EAP packet exchange (EAP-Request → EAP-Success) : No msg. in case of no error

- **[I:STA]** : STA sends
- **[O:STA]** : APC sends

2.2.1 Station Tracking History

Samsung Wireless Enterprise™

Trace the Station - Reassociation

```
16 TR_380A94ECCABA [2013-04-18 16:50:09.961.402] INF <dr_vlan1_114> Forwarded BOOTREPLY[DHCPACK] for 38:0a:94:ec:ca:ba to 70.31.216.220
17 TR_380A94ECCABA [2013-04-18 16:50:09.960.853] INF <dsub_dhcpr> DHCP PLD: 38:0a:94:ec:ca:ba station ip set 70.31.216.220
18 TR_380A94ECCABA [2013-04-18 16:50:09.960.682] INF <dsub_dhcpr> Another Station IP existed.(Ip=461fd8dc)
19 TR_380A94ECCABA [2013-04-18 16:50:09.960.449] INF <dr_vlan1_114>   [DHCPACK] received from dhcp server
20 TR_380A94ECCABA [2013-04-18 16:50:09.958.923] INF <dr_vlan1_114> Forwarded BOOTREQUEST[DHCPREQUEST] for 38:0a:94:ec:ca:ba to 70.30.150.30
21 TR_380A94ECCABA [2013-04-18 16:50:09.958.428] INF <dr_vlan1_114>   [DHCPREQUEST] received from dhcp client
22 TR_380A94ECCABA [2013-04-18 16:49:36.826.220] INF <security> STA(38:0a:94:ec:ca:ba) - RADIUS Acct: Interim Message Sent. Session 5167BFEC-0000004A
23 TR_380A94ECCABA [2013-04-18 16:49:36.826.133] INF <security> STA(38:0a:94:ec:ca:ba) - RADIUS
24 TR_380A94ECCABA [2013-04-18 16:49:36.825.555] INF <security> STA(38:0a:94:ec:ca:ba) - RADIUS
   tx=23612,5096397,0
25 TR_380A94ECCABA [2013-04-18 16:39:36.825.202] INF <security> STA(38:0a:94:ec:ca:ba) - RADIUS Acct: Interim Message Sent. Session 5167BFEC-0000004A
26 TR_380A94ECCABA [2013-04-18 16:39:36.825.114] INF <security> STA(38:0a:94:ec:ca:ba) - RADIUS Acct: Session 5167BFEC-0000004A Sent
27 TR_380A94ECCABA [2013-04-18 16:39:36.824.614] INF <security> STA(38:0a:94:ec:ca:ba) - RADIUS Acct: Session 5167BFEC-0000004A rx=23421,4639429,0
   tx=23106,4938730,0
28 TR_380A94ECCABA [2013-04-18 16:38:36.824.486] INF <security> STA(38:0a:94:ec:ca:ba) - STA-Info: Removed(0x556a3cfe10). wlan=1 ap=342 radio=2
29 TR_380A94ECCABA [2013-04-18 16:38:35.909.115] INF <security> STA(38:0a:94:ec:ca:ba) - Authenticated. user=jinwhan.lee vlan=114 qos=0 acl=<none>
   url=<none>
30 TR_380A94ECCABA [2013-04-18 16:38:35.908.748] INF <security> STA(38:0a:94:ec:ca:ba) - SetFlag: wlan=1 802.1x=1 dynVlan=1 aaa=1 vlan=114 qos=0
31 TR_380A94ECCABA [2013-04-18 16:38:35.908.400] INF <security> STA(38:0a:94:ec:ca:ba) - CAPWAP Send: SetSessionKey: seq=0x04010468 wlan=1 ap=358 radio=2
32 TR_380A94ECCABA [2013-04-18 16:38:35.908.129] INF <security> STA(38:0a:94:ec:ca:ba) - EAPOL-Key: Recv 4/4 msg of 4-way h/s
33 TR_380A94ECCABA [2013-04-18 16:38:35.900.552] INF <security> STA(38:0a:94:ec:ca:ba) - EAPOL-Key: Send 3/4 msg of 4-way h/s
34 TR_380A94ECCABA [2013-04-18 16:38:35.900.326] INF <security> STA(38:0a:94:ec:ca:ba) - EAPOL-Key: Recv 2/4 msg of 4-way h/s
35 TR_380A94ECCABA [2013-04-18 16:38:35.824.711] INF <security> STA(38:0a:94:ec:ca:ba) - EAPOL-Key: Send 1/4 msg of 4-way h/s
36 TR_380A94ECCABA [2013-04-18 16:38:35.824.587] INF <security> STA(38:0a:94:ec:ca:ba) - 802.1x Auth Skipped
37 TR_380A94ECCABA [2013-04-18 16:38:35.824.470] INF <security> STA(38:0a:94:ec:ca:ba) - Authentication started
38 TR_380A94ECCABA [2013-04-18 16:38:35.824.180] INF <security> STA(38:0a:94:ec:ca:ba) - STA Removed. count=1
39 TR_380A94ECCABA [2013-04-18 16:38:35.822.374] INF <security> STA(38:0a:94:ec:ca:ba) - PMK found. okc PMKID[6a,9b,87,..,5c,71,a5]
40 TR_380A94ECCABA [2013-04-18 16:38:35.822.264] INF <security> STA(38:0a:94:ec:ca:ba) - PMKSA-Add,OKC: apc=1 pmkid[6a,9b,87,..,5c,71,a5]
41 TR_380A94ECCABA [2013-04-18 16:38:35.820.622] INF <security> STA(38:0a:94:ec:ca:ba) - (Re)Assoc: PMKID[0][6a,9b,87,..,5c,71,a5]
42 TR_380A94ECCABA [2013-04-18 16:38:35.820.537] INF <security> STA(38:0a:94:ec:ca:ba) - (Re)Assoc: 1 PMKIDs Received
43 TR_380A94ECCABA [2013-04-18 16:38:35.820.425] INF <security> STA(38:0a:94:ec:ca:ba) - New STA-Info: Added. wlan=1
44 TR_380A94ECCABA [2013-04-18 16:38:35.817.850] INF <security> STA(38:0a:94:ec:ca:ba) - OKC: Started. wlan=1 ap=358 radio=2 prev-ap=342 prev-radio=2
45 TR_380A94ECCABA [2013-04-18 16:38:35.815.060] INF [I:STA] STA Moved - BSSs [342]:f4:d9:fb:37:67:11 to [358]:f4:d9:fb:37:22:b1
46 TR_380A94ECCABA [2013-04-18 16:38:35.814.070] INF <security> STA(38:0a:94:ec:ca:ba) - OKC MDS Recv: wlan=1 ap=358 radio=2
47 TR_380A94ECCABA [2013-04-18 16:38:35.813.155] INF [STA] Removed station(38:0a:94:ec:ca:ba) from BSS(f4:d9:fb:37:67:11)
48 TR_380A94ECCABA [2013-04-18 16:38:35.810.637] INF [I:STA] Reassociation - BSSID(f4:d9:fb:37:22:b1) STA(38:0a:94:ec:ca:ba)
49 TR_380A94ECCABA [2013-04-18 16:38:18.528.808] INF <security> STA(38:0a:94:ec:ca:ba) - STA-Info: Removed(0x556a771ff0). wlan=1 ap=365 radio=2
50 TR_380A94ECCABA [2013-04-18 16:38:17.627.273] INF <security> STA(38:0a:94:ec:ca:ba) - Authenticated. user=jinwhan.lee vlan=114 qos=0 acl=<none>
   url=<none>
```

RADIUS accounting Interim message (per 10 min.)

4 way-handshake

OKC starts

2.2.1 Station Tracking History

Samsung Wireless Enterprise™

Trace the Station – Authentication fails

- **Authentication fails due to the wrong ID/PASSWORD**
  - → **STA receives REJECT message from RADIUS server**
  - → **STA sends disassociation message and AP/APC releases the association session**

```
41 TR_B4629357DC45 [2013-04-29 15:37:21.992.885] INF <security> STA(b4:62:93:57:dc:45) - STA-Info: Removed(0x55662ea950)(ap_handle_timer). wlan=1 ap=224
   radio=1 auth-progress=0
42 TR_B4629357DC45 [2013-04-29 15:37:20.992.821] INF <security> STA(b4:62:93:57:dc:45) - STA PLD Deleted: Done. wlan=1 radio=1 ap=224
43 TR_B4629357DC45 [2013-04-29 15:37:20.983.623] INF [STA] Removed station(b4:62:93:57:dc:45) from BSS(f4:d9:fb:38:c9:42)
44 TR_B4629357DC45 [2013-04-29 15:37:20.982.799] INF <security> STA(b4:62:93:57:dc:45) - STA PLD: Deleted. id=404
45 TR_B4629357DC45 [2013-04-29 15:37:20.982.393] INF <security> STA(b4:62:93:57:dc:45) - AcctStat Update: rx=0 gigawords t
46 TR_B4629357DC45 [2013-04-29 15:37:20.982.309] INF <security> STA(b4:62:93:57:dc:45) - AcctStat Update: rx=0,0 bytes tx=
47 TR_B4629357DC45 [2013-04-29 15:37:20.982.213] INF <security> STA(b4:62:93:57:dc:45) - AcctStat Msg from AWMB: iface=A
48 TR_B4629357DC45 [2013-04-29 15:37:20.982.109] INF <security> STA(b4:62:93:57:dc:45) - AcctStat Msg from AWMB: wlan=1 rx=0,0 tx=7,1506
49 TR_B4629357DC45 [2013-04-29 15:37:20.981.342] INF [I:STA] Dissassociation - BSSID(f4:d9:fb:38:c9:42) STA(b4:62:93:57:dc:45)
50 TR_B4629357DC45 [2013-04-29 15:37:20.915.985] INF <security> STA(b4:62:93:57:dc:45) - EAP FAILURE2: 0 -> 1
51 TR_B4629357DC45 [2013-04-29 15:37:20.915.793] INF <security> STA(b4:62:93:57:dc:45) - RADIUS 802.1x Auth: Access Reject Received. id=174 code=3
52 TR_B4629357DC45 [2013-04-29 15:37:20.915.404] INF <security> STA(b4:62:93:57:dc:45) - RADIUS Recv[Auth]: ACCESS-REJECT msg. id=0xae len=44
53 TR_B4629357DC45 [2013-04-29 15:37:20.543.655] INF <security> STA(b4:62:93:57:dc:45) - 802.1x Recv: EAPOL-Start Received. pae-
   state=AUTH_PAE_AUTHENTICATING eap-state=EAP_IDLE
55 TR_B4629357DC45 [2013-04-29 15:37:20.523.972] INF <security> STA(b4:62:93:57:dc:45) - 802.1x Auth Started. reassoc=0
56 TR_B4629357DC45 [2013-04-29 15:37:20.523.825] INF <security> STA(b4:62:93:57:dc:45) - Authentication started
57 TR_B4629357DC45 [2013-04-29 15:37:20.521.191] INF <security> STA(b4:62:93:57:dc:45) - No PMKID Received from STA
58 TR_B4629357DC45 [2013-04-29 15:37:20.521.042] INF <security> STA(b4:62:93:57:dc:45) - New STA-Info: Added(0x55662ea950). wlan=1 ap=224 radio=1 count=1
59 TR_B4629357DC45 [2013-04-29 15:37:20.520.529] INF <security> STA(b4:62:93:57:dc:45) - STA PLD: Created. id=404
60 TR_B4629357DC45 [2013-04-29 15:37:20.518.621] INF [I:STA] Association - BSSID(f4:d9:fb:38:c9:42) STA(b4:62:93:57:dc:45)
```

STA receives REJECT and sends disassociation

REJECT is received from Authentication Server

2.2.1 Station Tracking History

Samsung Wireless Enterprise™

Trace the Station – Reassociation fails

- **STA does not response in the process of 4 way-handshake**
  - → **Reassociation fails**
  - → **These problems are usually caused by the WiFi driver's bugs of Android smartphone.**

```
154 TR_9463D100FB12 [2013-04-29 16:24:47.271.561] INF <security> STA(94:63:d1:00:fb:12) - STA PLD Deleted: Done. wlan=1 radio=2 ap=144
155 TR_9463D100FB12 [2013-04-29 16:24:47.271.561] INF <security> STA(94:63:d1:00:fb:12) - AcctStat Update: sta not found
156 TR_9463D100FB12 [2013-04-29 16:24:47.271.561] INF <security> STA(94:63:d1:00:fb:12) - AcctStat Msg from AWMB: iface=287 active=1,0x661128a0
157 TR_9463D100FB12 [2013-04-29 16:24:47.271.271] INF <security> STA(94:63:d1:00:fb:12) - AcctStat Msg from AWMB: wlan=1 rx=2619,486206 tx=3087,1188642
158 TR_9463D100FB12 [2013-04-29 16:24:47.269.693] INF [STA] Removed station(94:63:d1:00:fb:12) from BSS(f4:d9:fb:38:ae:11)
159 TR_9463D100FB12 [2013-04-29 16:24:47.269.220] INF <security> STA(94:63:d1:00:fb:12) - STA PLD: Deleted. id=93
160 TR_9463D100FB12 [2013-04-29 16:24:47.268.404] INF [O:STA] Dissasoc Sent - STA(94:63:d1:00:fb:12) reason:4WAY_HANDSHAKE_TIMEOUT.
161 TR_9463D100FB12 [2013-04-29 16:24:47.267.906] INF <security> STA(94:63:d1:00:fb:12) - STA-Info: Removed(0x5564a4e0f0)(ap_handle_timer). wlan=1 ap=144
    radio=2 auth-progress=0
162 TR_9463D100FB12 [2013-04-29 16:24:47.267.680] INF <security> STA(94:63:d1:00:fb:12) - Deauthenticated. reason=15 user=jw2002.shim wlan=1 ap=144 radio=2
163 TR_9463D100FB12 [2013-04-29 16:24:47.267.416] INF <security> STA(94:63:d1:00:fb:12) - Disconnect[WPA authenticator requests disconnect]:
    Deauth(15,4WAY_HANDSHAKE_TIMEOUT)
164 TR_9463D100FB12 [2013-04-29 16:24:47.267.222] INF <security> STA(94:63:d1:00:fb:12) - EAPOL-Key Timeout(WPA_PTK_PTKSTART,WPA_PTK_GROUP_IDLE)
165 TR_9463D100FB12 [2013-04-29 16:24:46.766.909] INF <security> STA(94:63:d1:00:fb:12) - EAPOL-Key: Send 1/4 msg of 4-way h/s
166 TR_9463D100FB12 [2013-04-29 16:24:46.766.754] INF <security> STA(94:63:d1:00:fb:12) - EAPOL-Key Timeout(WPA_PTK_PTKSTART,WPA_PTK_GROUP_IDLE)
168 TR_9463D100FB12 [2013-04-29 16:24:46.266.454] INF <security> STA(94:63:d1:00:fb:12) - EAPOL-Key: Send 1/4 msg of 4-way h/s
169 TR_9463D100FB12 [2013-04-29 16:24:46.266.314] INF <security> STA(94:63:d1:00:fb:12) - EAPOL-Key Timeout(WPA_PTK_PTKSTART,WPA_PTK_GROUP_IDLE)
170 TR_9463D100FB12 [2013-04-29 16:24:45.766.017] INF <security> STA(94:63:d1:00:fb:12) - EAPOL-Key: Send 1/4 msg of 4-way h/s
171 TR_9463D100FB12 [2013-04-29 16:24:45.765.861] INF <security> STA(94:63:d1:00:fb:12) - EAPOL-Key Timeout(WPA_PTK_PTKSTART,WPA_PTK_GROUP_IDLE)
    replay[00,00,00,00,00,00,00,01]
172 TR_9463D100FB12 [2013-04-29 16:24:45.565.611] INF <security> STA(94:63:d1:00:fb:12) - EAPOL-Key: Send 1/4 msg of 4-way h/s
173 TR_9463D100FB12 [2013-04-29 16:24:45.565.486] INF <security> STA(94:63:d1:00:fb:12) - 802.1x Auth Skipped
174 TR_9463D100FB12 [2013-04-29 16:24:45.565.362] INF <security> STA(94:63:d1:00:fb:12) - Authentication started
175 TR_9463D100FB12 [2013-04-29 16:24:45.563.806] INF <security> STA(94:63:d1:00:fb:12) - STA Removed(prune_account_stop). count=0 radio=2
176 TR_9463D100FB12 [2013-04-29 16:24:45.562.591] INF <security> STA(94:63:d1:00:fb:12) - PMK found.  PMKID[71,fa,8c,..,b9,4e,72]
177 TR_9463D100FB12 [2013-04-29 16:24:45.562.447] INF <security> STA(94:63:d1:00:fb:12) - (Re)Assoc: PMKID[0][71,fa,8c,..,b9,4e,72]
178 TR_9463D100FB12 [2013-04-29 16:24:45.562.354] INF <security> STA(94:63:d1:00:fb:12) - (Re)Assoc: 1 PMKIDs Received
179 TR_9463D100FB12 [2013-04-29 16:24:45.562.261] INF <security> STA(94:63:d1:00:fb:12) - New STA-Info: Added(0x5564a4e0f0). wlan=1 ap=144 radio=2 count=2
180 TR_9463D100FB12 [2013-04-29 16:24:45.562.034] INF <security> STA(94:63:d1:00:fb:12) - OKC: Started. wlan=1 ap=144 radio=2 prev-ap=158 prev-radio=2
181 TR_9463D100FB12 [2013-04-29 16:24:45.558.379] INF [I:STA] STA Moved - BSSs [158]:f4:d9:fb:3a:65:d1 to [144]:f4:d9:fb:38:ae:11
182 TR_9463D100FB12 [2013-04-29 16:24:45.558.138] INF <security> STA(94:63:d1:00:fb:12) - OKC MDS Recv: wlan=1 ap=144 radio=2
183 TR_9463D100FB12 [2013-04-29 16:24:45.557.459] INF [STA] Removed station(94:63:d1:00:fb:12) from BSS(f4:d9:fb:3a:65:d1)
184 TR_9463D100FB12 [2013-04-29 16:24:45.556.262] INF [I:STA] Reassociation - BSSID(f4:d9:fb:38:ae:11) STA(94:63:d1:00:fb:12)
```

APC sends disassociation

4th EAPOL timeout 500ms

3th EAPOL timeout 500ms

2th EAPOL timeout 500ms

1th EAPOL timeout 200ms

OKC starts

2.2.1 Station Tracking History

Samsung Wireless Enterprise™

Trace the Station – EAPOL-logoff

- **Android Smartphone send EAPOL-logoff message right after the successful association**
  → Sometimes occurred with Android Smartphone

```
518 TR_FCC734C0D912 [ 11:37:41.849.618] INF [I:STA] Dissassociation - BSSID(f4:d9:fb:37:bd:c2) STA(fc:c7:34:c0:d9:12)
                ...
529 TR_FCC734C0D912 [ 11:37:38.192.726] INF <security> STA(fc:c7:34:c0:d9:12) - RADIUS Acct[Stop](EAPOL-Logoff Recv): Stopped. Session 00008401-00000013
   wlan=1 ap=33 radio=1
530 TR_FCC734C0D912 [ 11:37:38.192.623] INF <security> STA(fc:c7:34:c0:d9:12) - RADIUS Acct[Stop]: Session 0000840
531 TR_FCC734C0D912 [ 11:37:38.192.189] INF <security> STA(fc:c7:34:c0:d9:12) - RADIUS Acct[Stop]: Session 00008401-000          1x=104,13215,0 tx=89,17784,0
532 TR_FCC734C0D912 [ 11:37:38.192.008] INF <security> STA(fc:c7:34:c0:d9:12) - 802.1x Recv: EAPOL-Logoff Received
533 TR_FCC734C0D912 [ 11:37:19.666.134] INF <security> STA(fc:c7:34:c0:d9:12) - RADIUS Acct[Start]: Started. Session 00008401-00000013 wlan=1 ap=33 radio=1
   ip=70.31.200.243
534 TR_FCC734C0D912 [ 11:37:19.657.663] INF <dr_vlan1_110> Forwarded BOOTREPLY[DHCPACK] for fc:c7:34:c0:d9:12 to 70.31.200.243
535 TR_FCC734C0D912 [ 11:37:19.656.992] INF <dsub_dhcpr> DHCP PLD: fc:c7:34:c0:d9:12 station ip set 70.31.200.243
536 TR_FCC734C0D912 [ 11:37:19.656.742] INF <dr_vlan1_110>   [DHCPACK] received from dhcp server
537 TR_FCC734C0D912 [ 11:37:19.656.169] INF <dr_vlan1_110> Forwarded BOOTREQUEST[DHCPREQUEST] for fc:c7:34:c0:d9:12 to 70.30.150.30
538 TR_FCC734C0D912 [ 11:37:19.655.749] INF <dr_vlan1_110>   [DHCPREQUEST] received from dhcp client
539 TR_FCC734C0D912 [ 11:37:19.653.499] INF <dr_vlan1_110> Forwarded BOOTREPLY[DHCPOFFER] for fc:c7:34:c0:d9:12 to 70.31.200.243
540 TR_FCC734C0D912 [ 11:37:19.653.142] INF <dr_vlan1_110>   [DHCPOFFER] received from dhcp server
541 TR_FCC734C0D912 [ 11:37:19.652.523] INF <dr_vlan1_110> Forwarded BOOTREQUEST[DHCPDISCOVER] for fc:c7:34:c0:d9:12 to 70.30.150.30
542 TR_FCC734C0D912 [ 11:37:19.652.019] INF <dr_vlan1_110>   [DHCPDISCOVER] received from dhcp client
543 TR_FCC734C0D912 [ 11:37:19.215.033] INF <security> STA(fc:c7:34:c0:d9:12) - PMKSA-Add: apc=1 pmkid[5f,35,1f,..,00,13,d9]
544 TR_FCC734C0D912 [ 11:37:19.212.616] INF <security> STA(fc:c7:34:c0:d9:12) - Authenticated. user=se13@uready.com vlan=110 qos=0 acl=<none> url=<none>
545 TR_FCC734C0D912 [ 11:37:19.212.317] INF <security> STA(fc:c7:34:c0:d9:12) - SetFlag[Auth]: wlan=1 802.1x=1 dynVlan=1 aaa=1 vlan=110 qos=0 ap=33 radio=1
546 TR_FCC734C0D912 [ 11:37:19.211.882] INF <security> STA(fc:c7:34:c0:d9:12) - CAPWAP Send: SetSessionKey: seq=0x02010b90 wlan=1 ap=33 radio=1
547 TR_FCC734C0D912 [ 11:37:19.211.658] INF <security> STA(fc:c7:34:c0:d9:12) - EAPOL-Key: Recv 4/4 msg of 4-way h/s
548 TR_FCC734C0D912 [ 11:37:19.209.222] INF <security> STA(fc:c7:34:c0:d9:12) - EAPOL-Key: Send 3/4 msg of 4-way h/s
549 TR_FCC734C0D912 [ 11:37:19.209.006] INF <security> STA(fc:c7:34:c0:d9:12) - EAPOL-Key: Recv 2/4 msg of 4-way h/s
550 TR_FCC734C0D912 [ 11:37:19.197.598] INF <security> STA(fc:c7:34:c0:d9:12) - EAPOL-Key: Send 1/4 msg of 4-way h/s
551 TR_FCC734C0D912 [ 11:37:19.196.302] INF <security> STA(fc:c7:34:c0:d9:12) - RADIUS Recv[Auth]: ACCESS-ACCEPT msg. id=0xe4 len=405
552 TR_FCC734C0D912 [ 11:37:18.947.503] INF <security> STA(fc:c7:34:c0:d9:12) - 802.1x Recv: EAPOL-Start Received. pae-state=AUTH_PAE_AUTHENTICATING eap-
   state=EAP_IDLE
553 TR_FCC734C0D912 [ 11:37:18.947.192] INF <security> STA(fc:c7:34:c0:d9:12) - 802.1x Auth Started. reassoc=0
554 TR_FCC734C0D912 [ 11:37:18.947.046] INF <security> STA(fc:c7:34:c0:d9:12) - Authentication started
555 TR_FCC734C0D912 [ 11:37:18.944.506] INF <security> STA(fc:c7:34:c0:d9:12) - No PMKID Received from STA
556 TR_FCC734C0D912 [ 11:37:18.944.400] INF <security> STA(fc:c7:34:c0:d9:12) - New STA-Info: Added(0x1205bbb20). wlan=1 ap=33 radio=1 count=1
557 TR_FCC734C0D912 [ 11:37:18.937.932] INF <security> STA(fc:c7:34:c0:d9:12) - STA PLD: Created. id=135
558 TR_FCC734C0D912 [ 11:37:18.936.161] INF [I:STA] Association - BSSID(f4:d9:fb:37:bd:c2) STA(fc:c7:34:c0:d9:12)
```

STA sends disassociation

STA sends EAPOL-logoff suddenly

Authentication Completed

Authentication Succeeded

2.2.2 Station Tracking Real-time

Samsung Wireless Enterprise™

Station Tracking List

```
WEC8500# show stationtracking station list

======= Station list =======

1 EC:55:F9:16:2F:17
2 EC:55:F9:99:60:60
3 B4:82:FE:E5:35:26
4 E8:39:DF:08:B1:77
======= Station list =======
```

2.2.2 Station Tracking Real-time

Samsung Wireless Enterprise™

AP Association

Command: wec8500/configure# stationtracking station D0:22:BE:72:F6:C5 on

```
WEC8500/configure# stationtracking station D0:22:BE:72:F6:C5 on
Station Debug On!!!
WEC8500/configure# *[2014-02-17:15:35:02.987] #TR_D022BE72F6C5-INF: unknown station
*[2014-02-17:15:35:02.990] #TR_D022BE72F6C5-INF: [I:STA] Association - BSSID(f4:d9:fb:3d:94:62) STA(d0:22:be:72:f6:c5)
*[2014-02-17:15:35:02.993] #TR_D022BE72F6C5-INF:  security  STA(d0:22:be:72:f6:c5) - STA PLD: Created. wlan=1 ap=1 radio=1 id=1
*[2014-02-17:15:35:02.999] #TR_D022BE72F6C5-INF:  security  STA(d0:22:be:72:f6:c5) - New STA-Info: Added(0x55680010a0). wlan=1 ap=1 radio=1 count=1
*[2014-02-17:15:35:02.999] #TR_D022BE72F6C5-INF:  security  STA(d0:22:be:72:f6:c5) - No PMKID Received from STA
*[2014-02-17:15:35:03.000] #TR_D022BE72F6C5-INF:  security  STA(d0:22:be:72:f6:c5) - EAPOL-Key: Send 1/4 msg of 4-way h/s. wlan=1 ap=1 radio=1
*[2014-02-17:15:35:03.005] #TR_D022BE72F6C5-INF:  security  STA(d0:22:be:72:f6:c5) - EAPOL-Key: Recv 2/4 msg of 4-way h/s. wlan=1 ap=1 radio=1
*[2014-02-17:15:35:03.005] #TR_D022BE72F6C5-INF:  security  STA(d0:22:be:72:f6:c5) - EAPOL-Key: Send 3/4 msg of 4-way h/s. wlan=1 ap=1 radio=1
*[2014-02-17:15:35:03.008] #TR_D022BE72F6C5-INF:  security  STA(d0:22:be:72:f6:c5) - EAPOL-Key: Recv 4/4 msg of 4-way h/s. wlan=1 ap=1 radio=1
*[2014-02-17:15:35:03.008] #TR_D022BE72F6C5-INF:  security  STA(d0:22:be:72:f6:c5) - CAPWAP Send: SetSessionKey: seq=0x00000000 apWlan=1 wlan=1 ap=1 radio=1
*[2014-02-17:15:35:03.008] #TR_D022BE72F6C5-INF:  security  STA(d0:22:be:72:f6:c5) - SetFlag[Auth]: wlan=1 802.1x=0 dynVlan=1 aaa=0 vlan=0 qos=0 ap=1 radio=1 prev-statu
s=0x802
*[2014-02-17:15:35:03.008] #TR_D022BE72F6C5-INF:  security  STA(d0:22:be:72:f6:c5) - SetFlag[Auth]: authType=3(PSK) authResult=1(Success) reauth=0
*[2014-02-17:15:35:03.009] #TR_D022BE72F6C5-INF:  security  STA(d0:22:be:72:f6:c5) - Authenticated
*[2014-02-17:15:35:03.010] #TR_D022BE72F6C5-INF: [STA_DATA] Auth Done - STA(d0:22:be:72:f6:c5) authType(CACHING Auth) authResult(Success)
*[2014-02-17:15:35:03.496] #TR_D022BE72F6C5-INF:  dr_vlan1_20    [DHCPDISCOVER] received from dhcp client
*[2014-02-17:15:35:03.496] #TR_D022BE72F6C5-DEB:  dsub_dhcpr  ## d0:22:be:72:f6:c5 station PLD info: onOff = 0, server_ip = 0x0
*[2014-02-17:15:35:03.497] #TR_D022BE72F6C5-DEB:  dr_vlan1_20  [vlan1.20- fallback]
*[2014-02-17:15:35:03.497] #TR_D022BE72F6C5-INF:  dr_vlan1_20  Forwarded BOOTREQUEST[DHCPDISCOVER] for d0:22:be:72:f6:c5 to 192.168.20.1
*[2014-02-17:15:35:03.746] #TR_D022BE72F6C5-INF:  dr_vlan1_20    [DHCPOFFER] received from dhcp server
*[2014-02-17:15:35:03.746] #TR_D022BE72F6C5-DEB:  dr_vlan1_20  DHCP PLD: Found Station.
*[2014-02-17:15:35:03.746] #TR_D022BE72F6C5-INF:  dr_vlan1_20  Forwarded BOOTREPLY[DHCPOFFER] for d0:22:be:72:f6:c5 to 192.168.20.38
*[2014-02-17:15:35:03.753] #TR_D022BE72F6C5-INF:  dr_vlan1_20    [DHCPREQUEST] received from dhcp client
*[2014-02-17:15:35:03.753] #TR_D022BE72F6C5-DEB:  dsub_dhcpr  ## d0:22:be:72:f6:c5 station PLD info: onOff = 0, server_ip = 0x0
*[2014-02-17:15:35:03.754] #TR_D022BE72F6C5-DEB:  dr_vlan1_20  [vlan1.20- fallback]
*[2014-02-17:15:35:03.754] #TR_D022BE72F6C5-INF:  dr_vlan1_20  Forwarded BOOTREQUEST[DHCPREQUEST] for d0:22:be:72:f6:c5 to 192.168.20.1
*[2014-02-17:15:35:03.755] #TR_D022BE72F6C5-INF:  dr_vlan1_20    [DHCPACK] received from dhcp server
*[2014-02-17:15:35:03.755] #TR_D022BE72F6C5-INF:  dsub_dhcpr  DHCP PLD: d0:22:be:72:f6:c5 station ip set 192.168.20.38
*[2014-02-17:15:35:03.756] #TR_D022BE72F6C5-DEB:  dr_vlan1_20  DHCP PLD: Updated station IP!
*[2014-02-17:15:35:03.756] #TR_D022BE72F6C5-INF:  dr_vlan1_20  Forwarded BOOTREPLY[DHCPACK] for d0:22:be:72:f6:c5 to 192.168.20.38
*[2014-02-17:15:35:03.766] #TR_D022BE72F6C5-INF:  security  STA(d0:22:be:72:f6:c5) - RADIUS Acct[Start]: server not configured. Session 00000401-00000004 wlan=1 ap=1 ra
dio=1
```

1. Association starts

2. 4 way handshake

3. Authentication Complete

4. DHCP process

5. Station gets an IP address

2.2.2 Station Tracking Real-time

Samsung Wireless Enterprise™

AP Disassociation

```
WEC8500/configure# *[2014-02-17:15:07:32.746] #TR_D022BE72F6C5-INF: [I:STA] Dissassociation Reason(8)- BSSID(f4:d9:fb:3d:94:62) STA(d0:22:be:72:f6:c5)
*[2014-02-17:15:07:32.748] #TR_D022BE72F6C5-INF:  security STA(d0:22:be:72:f6:c5) - STA PLD: Deleted. wlan=1 ap=1 radio=1 id=1
*[2014-02-17:15:07:32.748] #TR_D022BE72F6C5-INF: [STA] Removed station(d0:22:be:72:f6:c5) from BSS(f4:d9:fb:3d:94:62)
*[2014-02-17:15:07:32.750] #TR_D022BE72F6C5-INF:  security  STA(d0:22:be:72:f6:c5) - STA PLD Deleted: Done. wlan=1 radio=1 ap=1
*[2014-02-17:15:07:33.750] #TR_D022BE72F6C5-INF:  security  STA(d0:22:be:72:f6:c5) - STA-Info: Removed(0x5568002160)(ap_handle_timer). wlan=1 ap=1 radio=1 count=0 auth-
progress=0
```

Lab 17 -

Telnet into the APC and run a station trace

1. Connect your Cell Phone to an AP
2. Go to the about phone on your cell and retrieve your mobile phone MAC address
3. Telnet to the APC “192.168.xx.10”
4. Use this show command WEA8500#
    1. show stationtracking station list
    2. You should be able to find your mobile MAC address
5. Go to configure mode → WEA8500# configure terminal
    1. stationtracking station d0:22:be:be:e5:d6 on ***(Enter your MAC here)***
    2. Then disconnect and reconnect your mobile device

Samsung Wireless Enterprise™

Packet Capture

2.3.1 APC CLI Configuration

2.3.2 Operation Modes

2.3.1 APC CLI Configuration

Samsung Wireless Enterprise™

Remember that using a “?” will show you the list of available commands

```
npi_WEC8500# configure terminal
npi_WEC8500/configure# pcap
npi_WEC8500/configure/pcap# ?

      config-filter              Configure capture filter rule(active and remote mode only)
      config-ftp                 Configure FTP access information(active and passive mode only)
      enable-capwap-tunneling    Enable packet capture with CAPWAP tunneling
      exit                       Exit from pcap mode
      filtering-mode             Select filtering mode(active and remote mode only)
      operation-mode             Select operation mode
      save-mode                  Select file save mode(active and passive mode only)
      start-service              Start service(active and remote mode only)
      trigger-value              File save trigger values(active mode only)

      <cr>
```

2.3.1 APC CLI Configuration

Samsung Wireless Enterprise™

i. config-filter

1. (no) ap-mac : AP MAC
2. (no) enable-ap-mac : Enable/Disable
3. (no) station-mac : Station MAC
4. (no) enable-station-mac : Enable/Disable

ii. config-ftp: FTP server

1. ipv4-address : Server IPv4 address
2. login-id : Login ID & Password
3. remote-file-path : Remote File Save Location
4. stop-current-forcibly : FTP stop forcibly

iii. (no) enable-capwap-tunneling: include CAPWAP header or not(station-only, not-DTLS mode)

iv. filtering-mode [station-only | ap-only]

1. station-only : Use station MAC
2. ap-only : Use AP MAC

2.3.1 APC CLI Configuration

Samsung Wireless Enterprise™

i. **operation-mode** [active-mode | passive-mode | remote-mode]

1. Operation mode
   - A. active-mode : File create mode, it is saved on system or remote FTP server.
   - B. passive-mode : Voice Enhanced Module triggers specific station's packet capture file automatically.
   - C. remote-mode : Wireshark can receive packet capture information via remote packet capture protocol in real time.

ii. **save-mode** [local | ftp]: operation mode is needed to be active-mode

1. local : File will be saved system local disk
2. ftp : File will be transported ftp server

iii. **(no) start-service**

1. Different action with operation-mode
   - A. active-mode : start/stop packet capture
   - B. remote-mode : start waiting for Wireshark access
   - C. passive-mode : not used

Samsung Wireless Enterprise™

Operation Modes

2.3.2.1 Active Operation Mode

2.3.2.2 Remote Operation Mode

2.3.2 Operation Modes

Samsung Wireless Enterprise™

Operation-mode [active-mode | remote-mode]

- active-mode : File create mode, it is saved on the system or on a remote FTP server.
- remote-mode : Wireshark can be setup to receive the packet capture information via remote packet capture protocol in real time.

2.3.2.1 Active Operation Mode

Samsung Wireless Enterprise™

Active Operation Mode

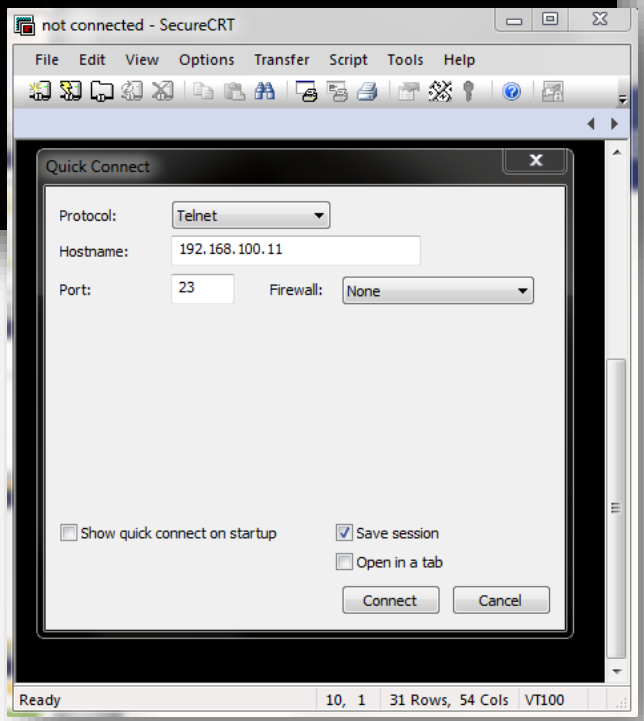
- Admin File Save (active mode)
- Save Mode
- Local Disk
- FTP Server Setup
- Trigger Value
- Packet Capturing
- Packet Capture Lab

2.3.2.1 Active Operation Mode

Samsung Wireless Enterprise™

Default User Name: samsung
Default Password: samsung

```
$=============================================================$
$WARNING: Unauthorized access to this system is forbidden and  $
$         will be prosecuted by law. By accessing this system, $
$         you agree that your actions may be monitored         $
$         if unauthorized usage is suspected.                  $
$=============================================================$

USERNAME : samsung
PASSWORD : **********

LAST LOGIN TIME : 2014-03-05 16:09:03
LOGIN FAIL COUNT : 1

npi_WEC8500#
```



Logging into the APC via CLI

2.3.2.1 Admin File Save (active mode)

Samsung Wireless Enterprise™

```
npi_WEC8500# show pcap current-config detail

 - Current Status    : Idle
 - Filtering Target  : Station
 - Operation Mode    : Admin File Save(active mode)
 - Save Mode         : Local Disk
 - CAPWAP Option     : Disabled
 - Trigger Values    : Period(3600 secs)/File Size(104

 - File Save Information(Local save mode)
        Local Path .....................................
        Disk Usage .....................................
        Saved File List(Last 10)
          | File Name                                          | Uploaded | Status              | Time
          |
          | apc_T03-04-10-46-36_RAB.pcap                       |      100 |           Completed |  03-04
 11:04:10 |

        Total File Saved Count ........................... 1
        Error Count ...................................... 0

 - Configured AP's MAC List
   No.        MAC Addr.          Filtering          Matched Count          Inbound Rate          Outbound Rate
 ===== ================== ========== ============================== ==================== ====================
=
 (empty)

 - Configured Station's MAC List
   No.        MAC Addr.          Filtering          Matched Count          Inbound Rate          Outbound Rate
 ===== ================== ========== ============================== ==================== ====================
=
 (empty)
```

Using the show command we can view the current pcap config detail

npi_WEC8500# show pcap current-config detail

2.3.2.1 Admin File Save (active mode)

Samsung Wireless Enterprise™

```
npi_WEC8500# show pcap current-config detail

 - Current Status    : Idle
 - Filtering Target  : Station
 - Operation Mode    : Admin File Save(active mode)
 - Save Mode         : Local Disk
 - CAPWAP Option     : Disabled
 - Trigger Values    : Period(3600 secs)/File Size(104857600 bytes)/Packet Count(4000000 packets)

 - File Save Information(Local save mode)
       Local Path ..................................... /user/log/se/pcap/
       Disk Usage ..................................... 1280KB/204800KB(0.00%)
       Saved File List(Last 10)
         | File Name                                                | Uploaded | Status              | Time
         |
         | apc_T03-04-10-46-36_RAB.pcap                             |      100 |           Completed |  03-04
11:04:10 |

       Total File Saved Count ..... 1
       Error Count .....

 - Configured AP's MAC List
  No.       MAC Addr.       Filtering          Matched Count              Inbound Rate         Outbound Rate
 ===== ================== ========== ============================== ================== ==================
=
 (empty)

 - Configured Station's MAC List
  No.       MAC Addr.       Filtering          Matched Count              Inbound Rate         Outbound Rate
 ===== ================== ========== ============================== ================== ==================
=
 (empty)
```

Check the current operation mode

2.3.2.1 Admin File Save (active mode)

Samsung Wireless Enterprise™

```
npi_WEC8500# configure terminal
npi_WEC8500/configure# pcap
npi_WEC8500/configure/pcap# operation-mode active-mode
The current operation mode is active-mode.
npi_WEC8500/configure/pcap# show pcap current-config detail

 - Current Status    : Idle
   Filtering Target : Station
 - Operation Mode    : Admin File Save(active mode)
 - Save Mode         : Local Disk
 - CAPWAP Option     : Disabled
 - Trigger Values    : Period(3600 secs)/File Size(104857600 bytes)/Packet Count(4000000 packets)

 - File Save Information(Local save mode)
        Local Path ..... ............................. /user/log/se/pcap/
        Disk Usage ..... ............................. 1280KB/204800KB(0.00%)
        Saved File List(Last 10)
          | File Name                                                  | Uploaded | Status                | Time
          |
          | apc_T03-04-10-46-36_RAB.pcap                                                                  |  03-04
 11:04:10 |

        Total File Saved Count ....................... 1
        Error Count .................................. 0

 - Configured AP's MAC List
  No.        MAC Addr.         Filtering          Matched Count              Inbound Rate          Outbound Rate
 ===== ==================== ========== ============================== ==================== ====================
=
 (empty)

 - Configured Station's MAC List
  No.        MAC Addr.         Filtering          Matched Count              Inbound Rate          Outbound Rate
 ===== ==================== ========== ============================== ==================== ====================
=
 (empty)
```

This mode can store the pcap file locally on the APC or send the pcap to a FTP Server

2.3.2.1 Save Mode

```
npi_WEC8500/configure/pcap# save-mode ?
  local                         Captured date is saved in local disk
  ftp                           Captured date is sent to remote storage using FTP
npi_WEC8500/configure/pcap# save-mode
```


npi_WEC8500/configure/pcap# save-mode ?
  local   Captured date is saved in local disk
  ftp   Captured date is sent to remote storage using FTP
npi_WEC8500/configure/pcap# save-mode

2.3.2.1 Local Disk

Samsung Wireless Enterprise™

```
npi_WEC8500/configure/pcap# start-service
Service is started successfully.
npi_WEC8500/configure/pcap# show pcap current-config detail

 - Current Status    : Now capturing
 - Filtering Target  : Station
 - Operation Mode    : Admin File Save(active mode)
 - Save Mode         : Local Disk
 - CAPWAP Option     : Disabled
 - Trigger Values    : Period(3600 secs)/File Size(104857600 bytes)/Packet Count(4000000 packets)

 - Current Info to Save File
       Seconds to Trigger ............................... 2/3600
       Bytes to Trigger ................................. 0/104857600
       Packets to Trigger ............................... 0/4000000

 - File Save Information(Local save mode)
       Local Path ....................................... /user/log/se/pcap/
       Disk Usage ....................................... 8KB/204800KB(0.00%)
       Saved File List(Last 10)
         | File Name                                                | Uploaded | Status              | Time              |
         | apc_T03-04-10-46-36_RAB.pcap                             |      100 |           Completed |  03-04 11:04:10 |
         | apc_T03-17-14-10-59_RAB.pcap                             |      100 |           Completed |  03-17 14:12:11 |
         | apc_T03-17-14-19-27_RAB.pcap                             |      100 |           Completed |  03-17 14:19:49 |

       Total File Saved Count ........................... 3
       Error Count ...................................... 0

 - Configured AP's MAC List
  No.        MAC Addr.        Filtering          Matched Count            Inbound Rate          Outbound Rate
 ===== ================== ========== ============================== ==================== ====================
     1   F4:D9:FB:3D:C4:84   -------->ON                        0              0.0 kbps              0.0 kbps
         ID       Prf.              AP Name                 IPv4 Addr
        ------ ------------ ---------------------------- ---------------
             1         ap_1                   npi_Lab_AP  192.168.10.100

 - Configured Station's MAC List
  No.        MAC Addr.        Filtering          Matched Count            Inbound Rate          Outbound Rate
 ===== ================== ========== ============================== ==================== ====================
     1   1C:99:4C:AB:29:F8   -------->ON                      282              0.0 kbps              0.0 kbps
               AP   WN               SSID                 IPv4 Addr
              ---- ---- ---------------------------- ---------------
                 1    1                 SamsungNPI 192.168.100.129
```

This capture will be saved to the local disk

npi_WEC8500/configure/pcap# start-service
Service is started successfully.
npi_WEC8500/configure/pcap# show pcap current-config detail

2.3.2.1 Local Disk

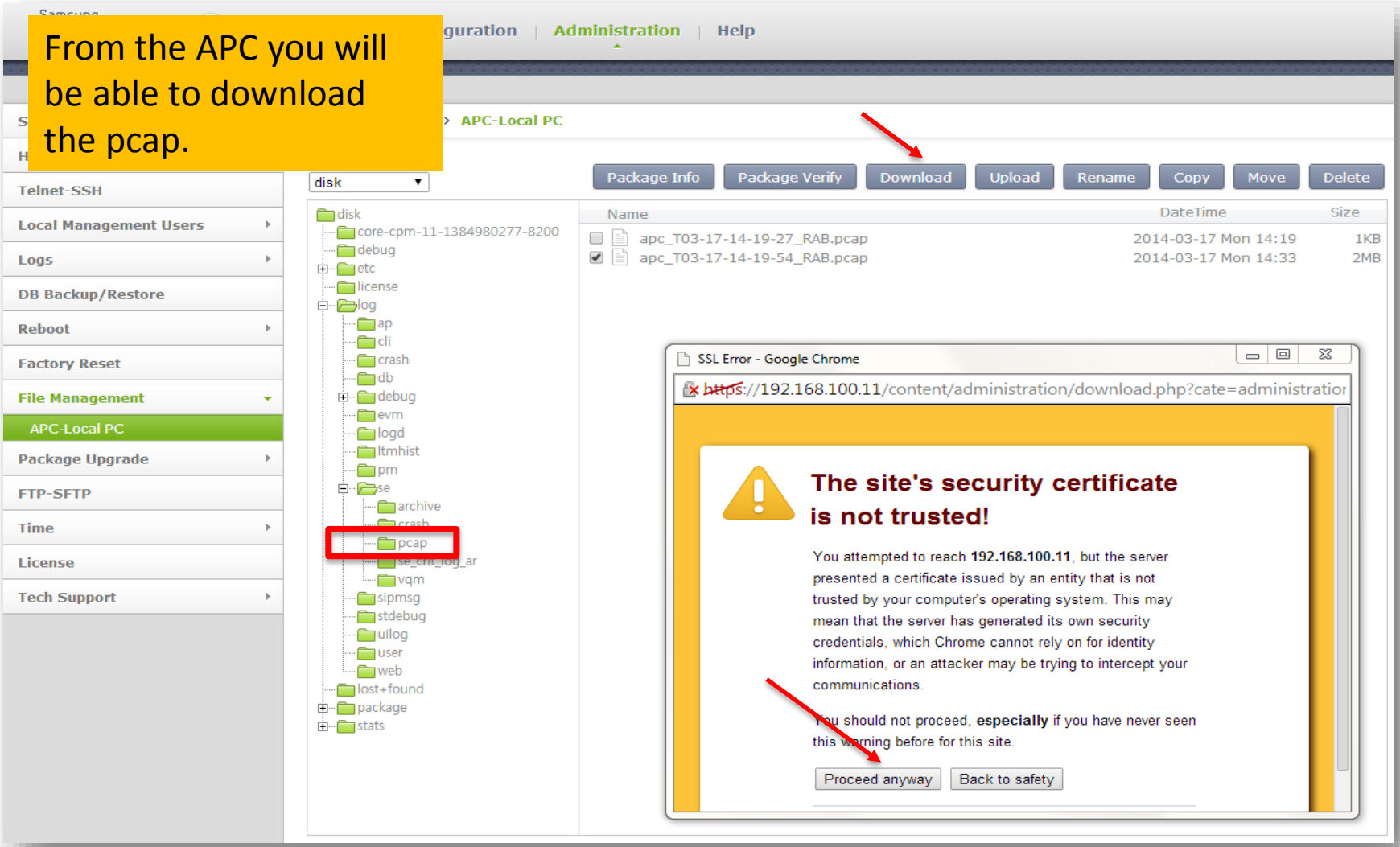
Samsung Wireless Enterprise™

After you stop the service, the file will be saved on the disk.
Here is the Saved File List

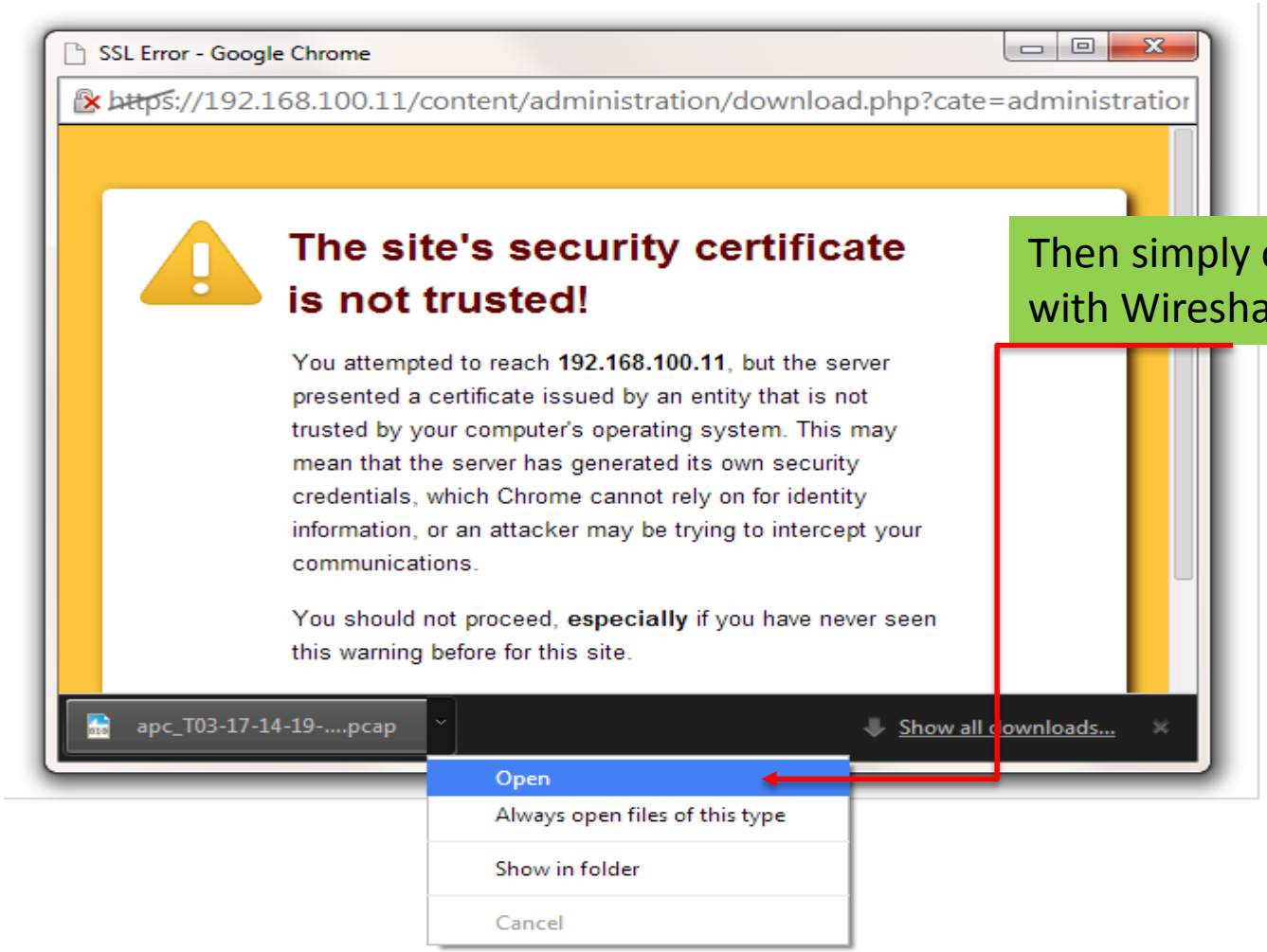
npi_WEC8500/configure/pcap# no start-service
Service is stopped successfully.
npi_WEC8500/configure/pcap# show pcap current-config detail

2.3.2.1 Local Disk

From the APC you will be able to download the pcap.



2.3.2.1 Local Disk



2.3.2.1 FTP Server Setup

Samsung Wireless Enterprise™

```
npi_WEC8500/configure/pcap# save-mode ftp
The current save mode is ftp.
npi_WEC8500/configure/pcap# show pcap current-config detail

- Current Status    : Idle
- Filtering Target  : Station
- Operation Mode    : Admin File Save(active mode)
- Save Mode         : FTP
- CAPWAP Option     : Disabled
- Trigger Values    : Period(3600 secs)/File Size(104857600 bytes)/Packet Count(4000000 packets)

- File Save Infomation(FTP save mode)
       IPv4 Address ..................................... 192.168.0.101
       Login Name/Password .............................. admin/admin
       Remote Path ...................................... ~/pcapFtp/
       Uploaded File List(Last 10)
         | File Name                                                | Uploaded | Status              | Time           |
         | apc_T03-04-10-46-36_RAB.pcap                             |      100 |           Completed |  03-04 11:04:10 |
         | apc_T03-17-14-10-59_RAB.pcap                             |      100 |           Completed |  03-17 14:12:11 |
         | apc_T03-17-14-19-27_RAB.pcap                             |      100 |           Completed |  03-17 14:19:49 |
         | apc_T03-17-14-19-54_RAB.pcap                             |      100 |           Completed |  03-17 14:33:36 |

       Total Uploaded Count ............................. 4
       Error Count ...................................... 0

- Configured AP's MAC List
 No.        MAC Addr.        Filtering          Matched Count            Inbound Rate         Outbound Rate
===== ================== ========== ============================== ==================== ====================
    1   F4:D9:FB:3D:C4:84   -------->ON                        0              0.0 kbps             0.0 kbps
        ID       Prf.               AP Name                IPv4 Addr
       ------ ---------- ---------------------------- ---------------
            1         ap_1                   npi_Lab_AP  192.168.10.100

- Configured Station's MAC List
 No.        MAC Addr.        Filtering          Matched Count            Inbound Rate         Outbound Rate
===== ================== ========== ============================== ==================== ====================
    1   1C:99:4C:AB:29:F8   --------->ON                    3,482              0.0 kbps             0.0 kbps
              AP   WN              SSID                  IPv4 Addr
             ---- ---- ------------------------------ ---------------
                1    1                    SamsungNPI 192.168.100.129
```

npi_WEC8500/configure/pcap# save-mode ftp
The current save mode is ftp.
npi_WEC8500/configure/pcap# show pcap current-config detail

2.3.2.1 FTP Server Setup

Samsung Wireless Enterprise™

```
npi_WEC8500/configure/pcap#
npi_WEC8500/configure/pcap#
npi_WEC8500/configure/pcap# config-ftp
npi_WEC8500/configure/pcap/config-ftp# ?

      exit                          Exit from config-ftp mode
      ipv4-address                  FTP server's address
      login-id                      FTP login ID
      remote-file-path              Remote file path
      stop-current-forcibly         Stop the current FTP uploading forcibly
```

npi_WEC8500/configure/pcap/config-ftp# ipv4-address 192.168.100.99
FTP server IPv4 address is configured(192.168.100.99).
npi_WEC8500/configure/pcap/config-ftp# login-id samsung samsung*#
FTP Login ID(samsung) and Password(samsung) is configured.
npi_WEC8500/configure/pcap/config-ftp# remote-file-path Traces/
FTP Remote Path(Traces/) is configured.
npi_WEC8500/configure/pcap/config-ftp# exit
npi_WEC8500/configure/pcap# start-service

2.3.2.1 FTP Server Setup

Samsung Wireless Enterprise™

```
npi_WEC8500/configure/pcap# start-service
Service is started successfully.
npi_WEC8500/configure/pcap# show pcap current-config detail

 - Current Status    : Now capturing
 - Filtering Target  : Station
 - Operation Mode    : Admin File Save(active mode)
 - Save Mode         : FTP
 - CAPWAP Option     : Disabled
 - Trigger Values    : Period(60 secs)/File Size(1048576 bytes)/Packet C

 - Current Info to Save File
       Seconds to Trigger ............................... 9/60
       Bytes to Trigger ................................. 0/1048576
       Packets to Trigger ............................... 0/50000

 - File Save Infomation(FTP save mode)
       IPv4 Address ..................................... 192.168.100.99
       Login Name/Password .............................. samsung/samsung*#
       Remote Path ...................................... Traces/
       Uploaded File List(Last 10)
          | File Name                                                | Uploaded | Status                | Time           |
          | apc_T03-19-05-35-17_RTM.pcap                             |        0 |   Cannot access file  |  03-19 05:36:38 |
          | apc_T03-19-06-09-49_RTM.pcap                             |      100 |              Completed |  03-19 06:10:50 |
          | apc_T03-19-06-14-56_RTM.pcap                             |      100 |              Completed |  03-19 06:15:57 |
          | apc_T03-19-08-19-53_RTM.pcap                             |      100 |              Completed |  03-19 08:20:55 |
          | apc_T03-19-08-32-08_RTM.pcap                             |      100 |              Completed |  03-19 08:33:08 |
          | apc_T03-19-04-58-22_RTM.pcap                             |        0 |   Cannot access file  |  03-19 04:59:43 |
          | apc_T03-19-05-04-37_RTM.pcap                             |      100 |              Completed |  03-19 05:05:38 |
          | apc_T03-19-05-07-21_RTM.pcap                             |        0 |   Cannot access file  |  03-19 05:08:43 |
          | apc_T03-19-05-09-40_RTM.pcap                             |        0 |   Cannot access file  |  03-19 05:11:02 |
          | apc_T03-19-05-11-41_RTM.pcap                             |        0 |   Cannot access file  |  03-19 05:13:02 |

       Total Uploaded Count ............................. 9
       Error Count ...................................... 46

 - Configured AP's MAC List
  No.        MAC Addr.        Filtering          Matched Count              Inbound Rate          Outbound Rate
 ===== ================== =========== ============================== ==================== ====================
 (empty)

 - Configured Station's MAC List
  No.        MAC Addr.        Filtering          Matched Count              Inbound Rate          Outbound Rate
 ===== ================== =========== ============================== ==================== ====================
     1   1C:99:4C:AB:29:F8   -------->ON                      155,420              0.0 kbps              0.0 kbps
              AP   WN               SSID                    IPv4 Addr
             ---- ---- ------------------------------ ---------------
                1    1                    SamsungNPI 192.168.100.129
```

Once the Trigger Period expires the pcap will be sent to your FTP Server.
You can also force this by stopping the service

2.3.2.1 Trigger Value

Samsung Wireless Enterprise™

```
npi_WEC8500/configure# pcap
npi_WEC8500/configure/pcap# trigger-value ?
  60 - 3600                          Period second (60 - 3600)

npi_WEC8500/configure/pcap# trigger-value 60 ?
  500 - 102400                       File size (KBytes: 500 - 102400)

npi_WEC8500/configure/pcap# trigger-value 60 500 ?
  5000 - 4000000                     Packet count (5000 - 4000000)

npi_WEC8500/configure/pcap# trigger-value 60 500 50000
```

```
npi_WEC8500/configure# pcap
npi_WEC8500/configure/pcap# trigger-value ?
 60 - 3600                Period second (60 - 3600)
npi_WEC8500/configure/pcap# trigger-value 60 ?
 500 - 102400             File size (KBytes: 500 - 102400)
npi_WEC8500/configure/pcap# trigger-value 60 500 ?
 5000 - 4000000           Packet count (5000 - 4000000)
npi_WEC8500/configure/pcap# trigger-value 60 500 50000
```

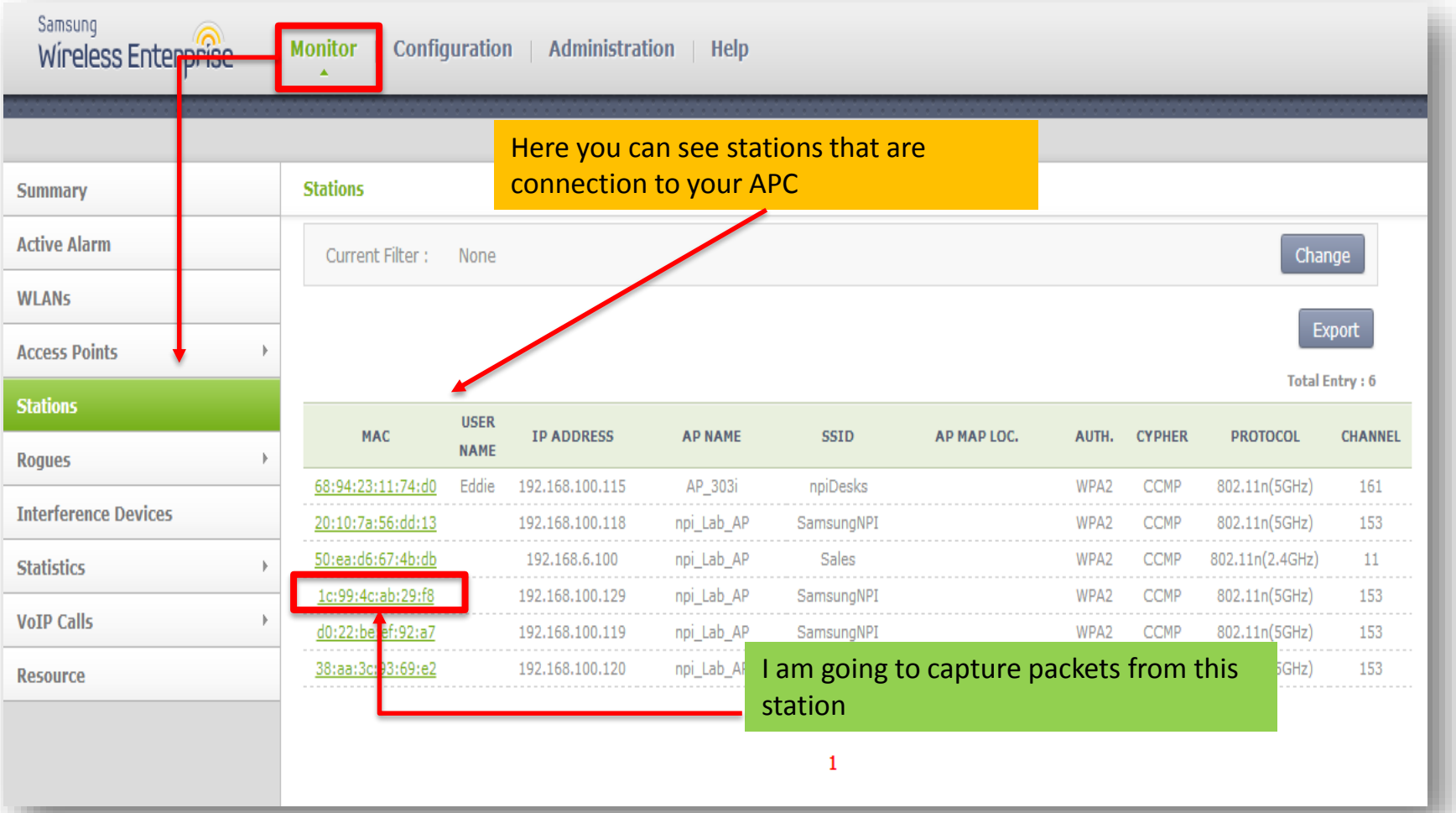
Packet Capturing

Samsung Wireless Enterprise™

Packet Capturing Steps

- MAC of a Station
- MAC of a Access Point
- Configuring Filtering Mode
- Operation Mode
- Save Mode
- Setup Trigger Value
- Start the Service

MAC of a Station



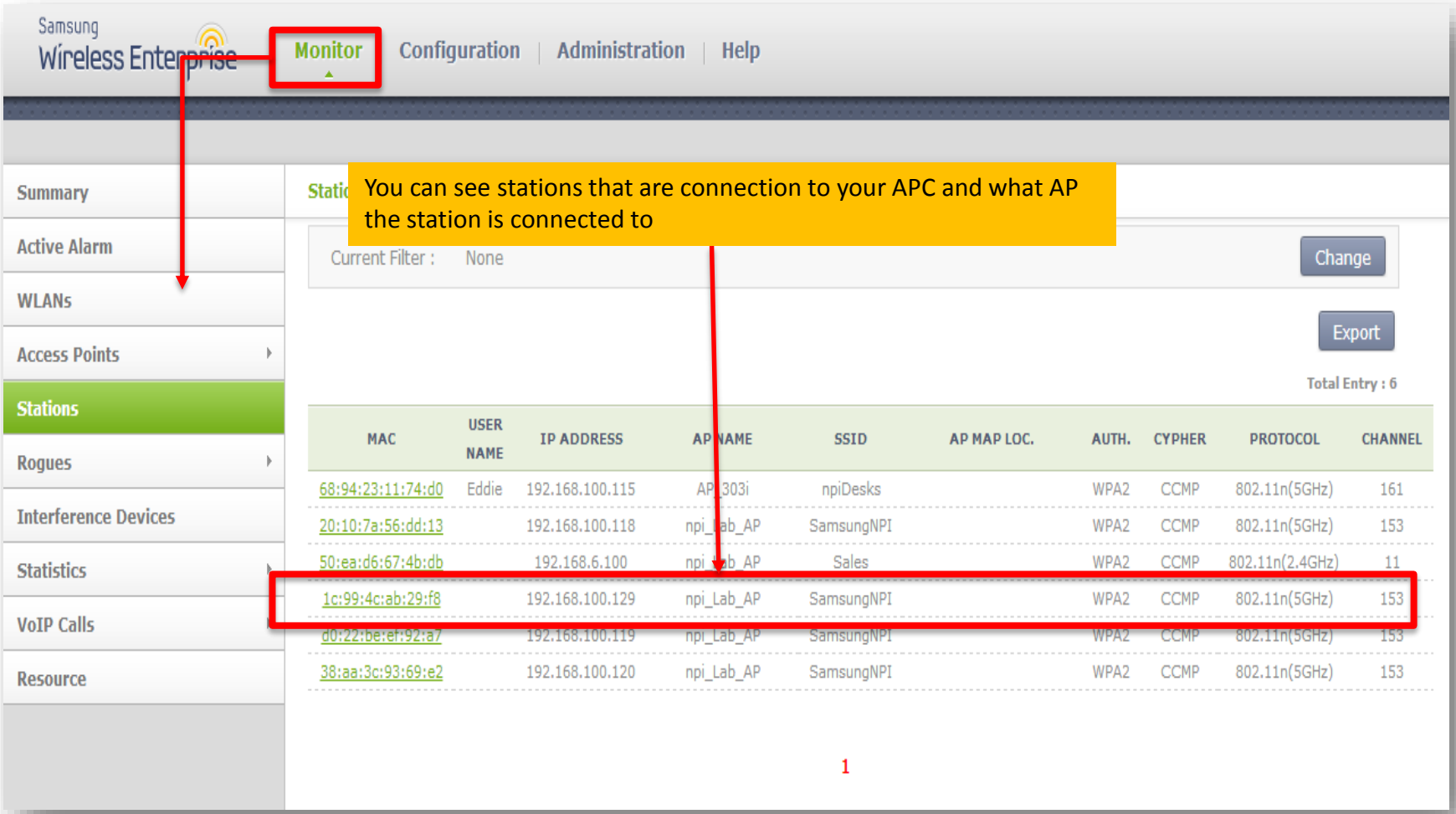
MAC of a Station

Samsung Wireless Enterprise™

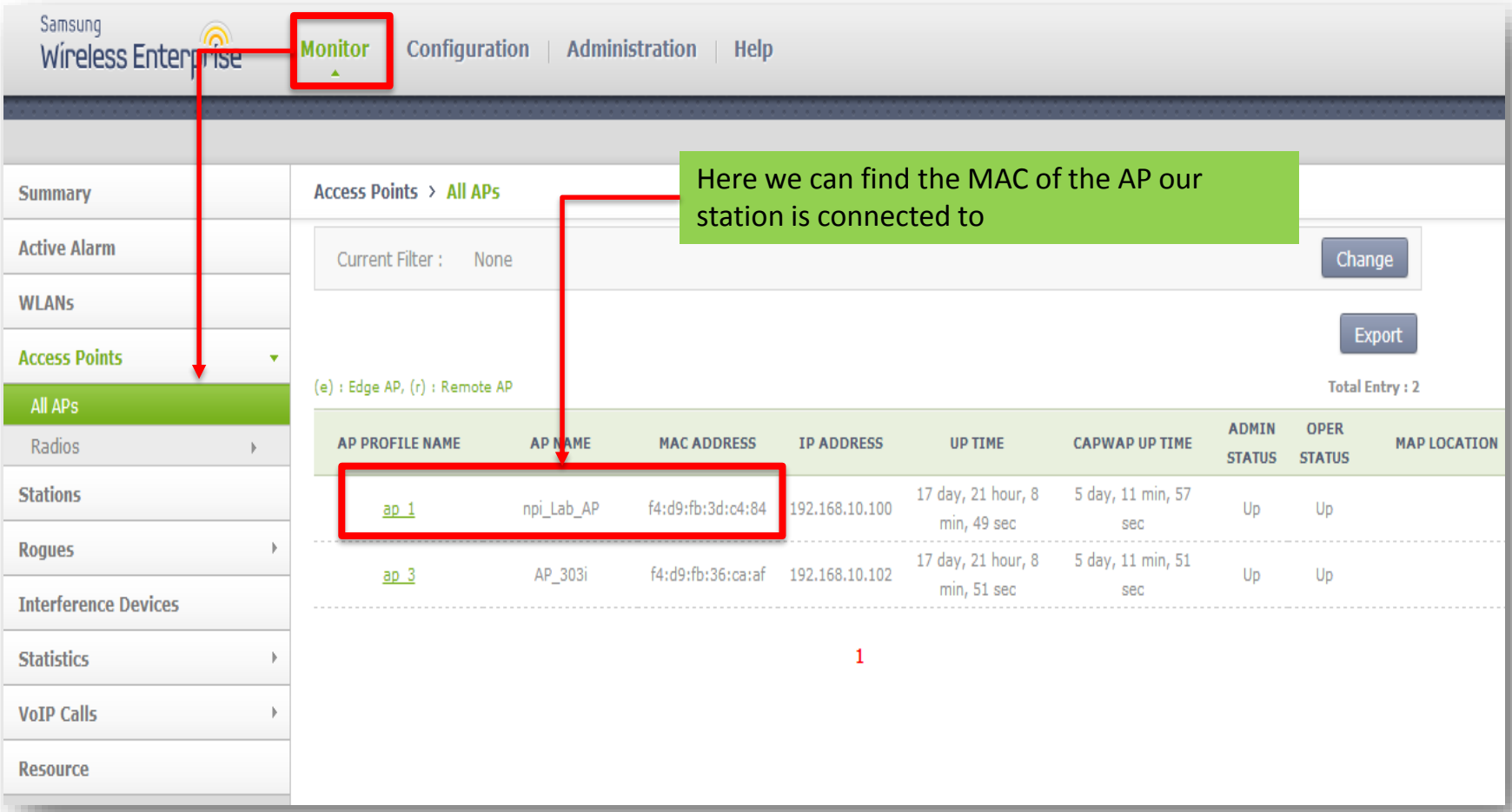
```
npi_WEC8500/configure/pcap# config-filter
npi_WEC8500/configure/pcap/config-filter# station-mac 1c:99:4c:ab:29:f8
The MAC value is added successfully.
npi_WEC8500/configure/pcap/config-filter# show pcap current-config detail

 - Current Status    : Idle
 - Filtering Target  : Station
 - Operation Mode    : Remote Packet Capture(remote mode)

 - Configured AP's MAC List
  No.        MAC Addr.        Filtering          Matched Count             Inbound Rate          Outbound Rate
 ===== ==================== ========== ============================== ==================== ====================
 (empty)

 - Configured Station's MAC List
  No.        MAC Addr.        Filtering          Matched Count             Inbound Rate          Outbound Rate
 ===== ==================== ========== ============================== ==================== ====================
    1   1C:99:4C:AB:29:F8   OFF<-------                              0              0.0 kbps              0.0 kbps
              AP   WN                SSID                    IPv4 Addr
             ---- ---- ------------------------------ ---------------
                1    1                       SamsungNPI 192.168.100.129
```

npi_WEC8500/configure/pcap# config-filter
npi_WEC8500/configure/pcap/config-filter# station-mac 1c:99:4c:ab:29:f8
npi_WEC8500/configure/pcap/config-filter# show pcap current-config detail

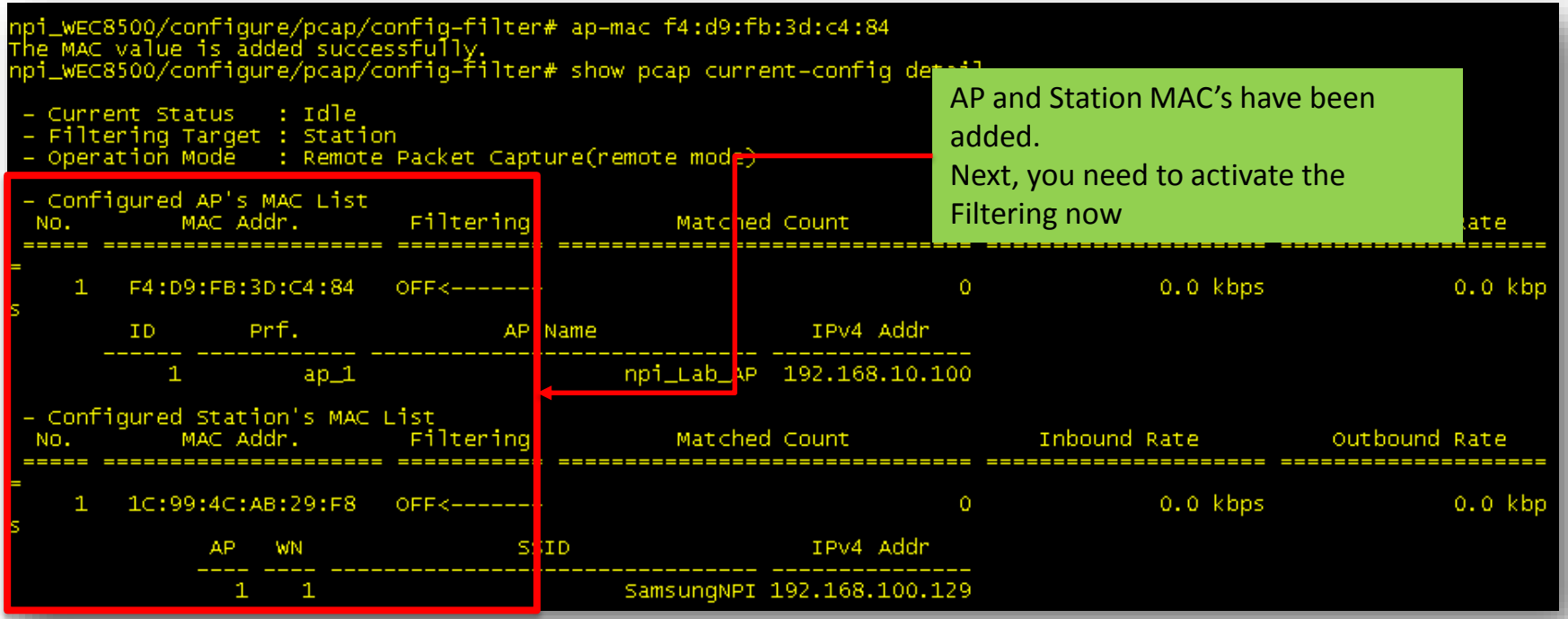
MAC of a Station



MAC of a Access Point



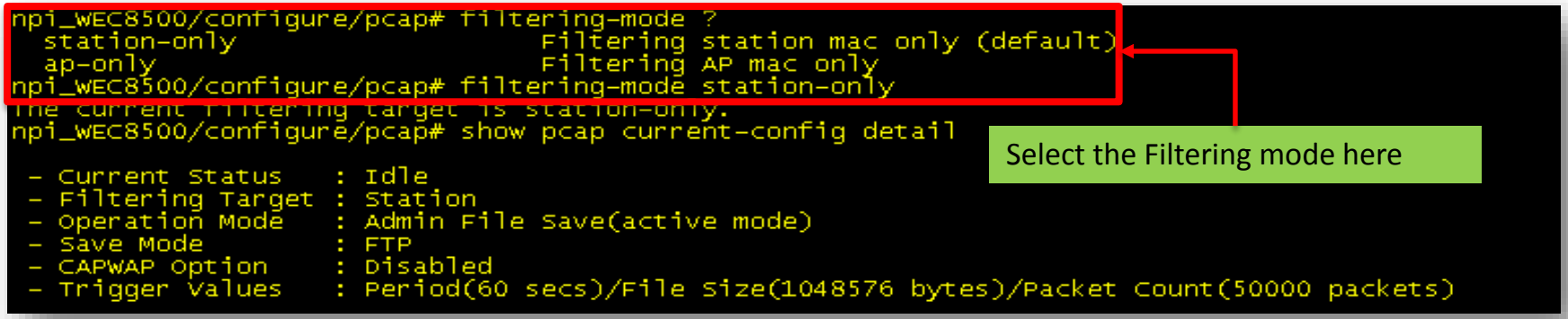
MAC of a Access Point



npi_WEC8500/configure/pcap/config-filter# ap-mac f4:d9:fb:3d:c4:84
npi_WEC8500/configure/pcap/config-filter# show pcap current-config detail

Configuring Filtering Mode

Samsung Wireless Enterprise™

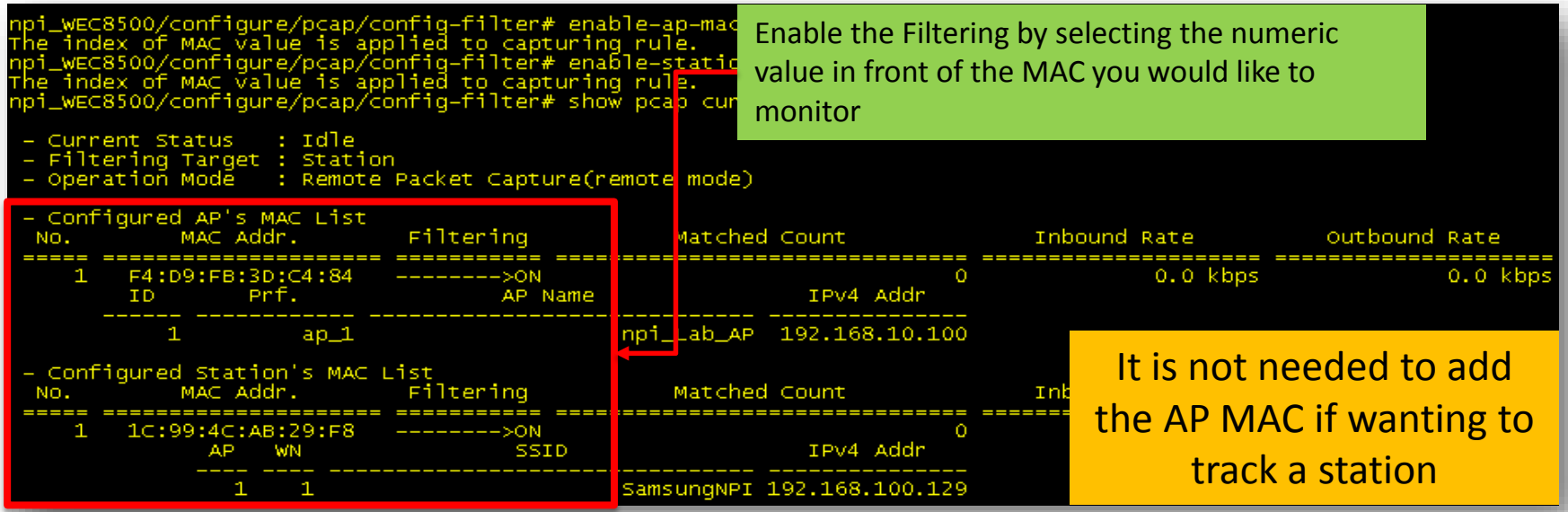



```
npi_WEC8500/configure/pcap# filtering-mode ?
  station-only                  Filtering station mac only (default)
  ap-only                       Filtering AP mac only
npi_WEC8500/configure/pcap# filtering-mode station-only
The current filtering target is station-only.
npi_WEC8500/configure/pcap# show pcap current-config detail
```

station-only *Filtering station mac only (default)*

ap-only *Filtering AP mac only*

Configuring Filtering Mode




```
npi_WEC8500/configure/pcap/config-filter# enable-ap-mac 1
The index of MAC value is applied to capturing rule.
npi_WEC8500/configure/pcap/config-filter# enable-station-mac 1
The index of MAC value is applied to capturing rule.
npi_WEC8500/configure/pcap/config-filter# show pcap current-config detail
```

Trigger Value

Samsung Wireless Enterprise™

```
npi_WEC8500/configure# pcap
npi_WEC8500/configure/pcap# trigger-value ?
  60 - 3600                       Period second (60 - 3600)

npi_WEC8500/configure/pcap# trigger-value 60 ?
  500 - 102400                    File size (KBytes: 500 - 102400)

npi_WEC8500/configure/pcap# trigger-value 60 500 ?
  5000 - 4000000                  Packet count (5000 - 4000000)

npi_WEC8500/configure/pcap# trigger-value 60 500 50000
```

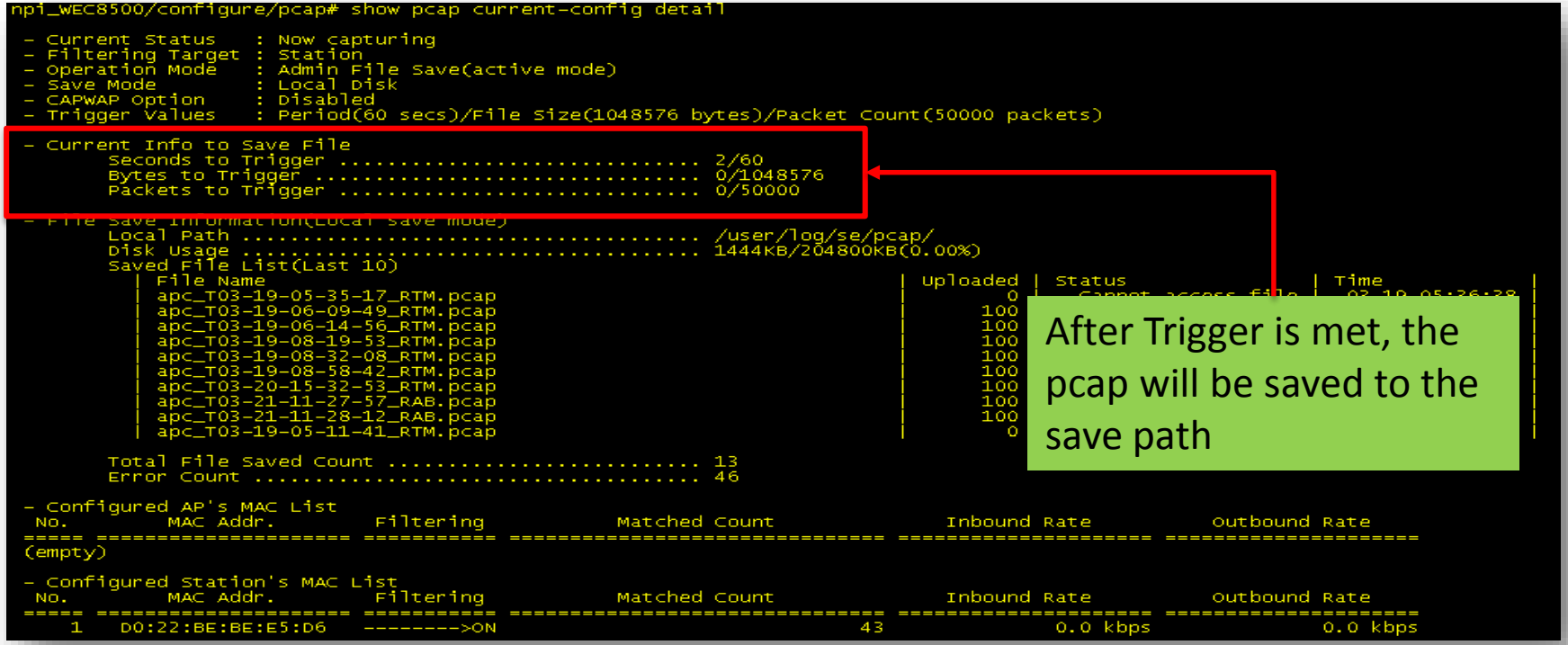
```
npi_WEC8500/configure# pcap
npi_WEC8500/configure/pcap# trigger-value ?
 60 - 3600                Period second (60 - 3600)
npi_WEC8500/configure/pcap# trigger-value 60 ?
 500 - 102400             File size (KBytes: 500 - 102400)
npi_WEC8500/configure/pcap# trigger-value 60 500 ?
 5000 - 4000000           Packet count (5000 - 4000000)
npi_WEC8500/configure/pcap# trigger-value 60 500 50000
```

Trigger Value

```
npi_WEC8500/configure/pcap# trigger-value 60 1024 50000
Trigger values are configured(60/1024/50000).
npi_WEC8500/configure/pcap# show pcap current-config detail

 - Current Status    : Idle
 - Filtering Target  : Station
 - Operation Mode    : Admin File Save(active mode)
 - Save Mode         : Local Disk
 - CAPWAP Option     : Disabled
 - Trigger Values    : Period(60 secs)/File Size(1048576 bytes)/Packet Count(50000 packets)

 - File Save Information(Local save mode)
       Local Path ..................................... /user/log/se/pcap/
       Disk Usage ..................................... 1436KB/204800KB(0.00%)
```

Trigger Value has been set

Start the Service




```
npi_WEC8500/configure/pcap/config-filter# exit
npi_WEC8500/configure/pcap# start-service
Service is started successfully.
npi_WEC8500/configure/pcap# show pcap current-config detail
```

Lab 18 – (1/2)

Telnet into the APC and get a pcap of a connected device.

The pcap should be stored locally and retrieved to the computer desktop

Connect a station to a WLAN
Find the MAC address of that device
Add the station here
npi_WEC8500# configure terminal
npi_WEC8500/configure# pcap
npi_WEC8500/configure/pcap# config-filter
npi_WEC8500/configure/pcap/config-filter# station-mac D0:22:BE:BE:E5:D6
Set Filtering to ON
npi_WEC8500/configure/pcap/config-filter# enable-station-mac 1
npi_WEC8500/configure/pcap/config-filter# exit
Select Operation Mode
npi_WEC8500/configure/pcap# operation-mode active-mode
Select Save Mode
npi_WEC8500/configure/pcap# save-mode local
Set Trigger Value
npi_WEC8500/configure/pcap# trigger-value 60 1024 50000

Samsung Wireless Enterprise™

Lab 18 – (1/2)

Telnet into the APC and get a pcap of a connected device.

The pcap should be stored locally and retrieved to the computer desktop

Check the current config

npi_WEC8500/configure/pcap# show pcap current-config detail

2.3.2.2 Remote Operation Mode

Samsung Wireless Enterprise™

Remote Operation Mode

- Remote Packet Capture
- Select Operation Mode
- Configuring the MAC of a station
- Configuring AP MAC address
- Configuring Filtering Mode
- Starting the Service
- Computer Setup
- Stopping the Service

Samsung Wireless Enterprise™

Remote Packet Capture w/Wire-Shark

- The APC can capture a packet exchanged between the wireless terminals on a remote PC in real-time by using the remote packet capture protocol.

2.3.2.2 Remote Packet Capture

Samsung Wireless Enterprise™

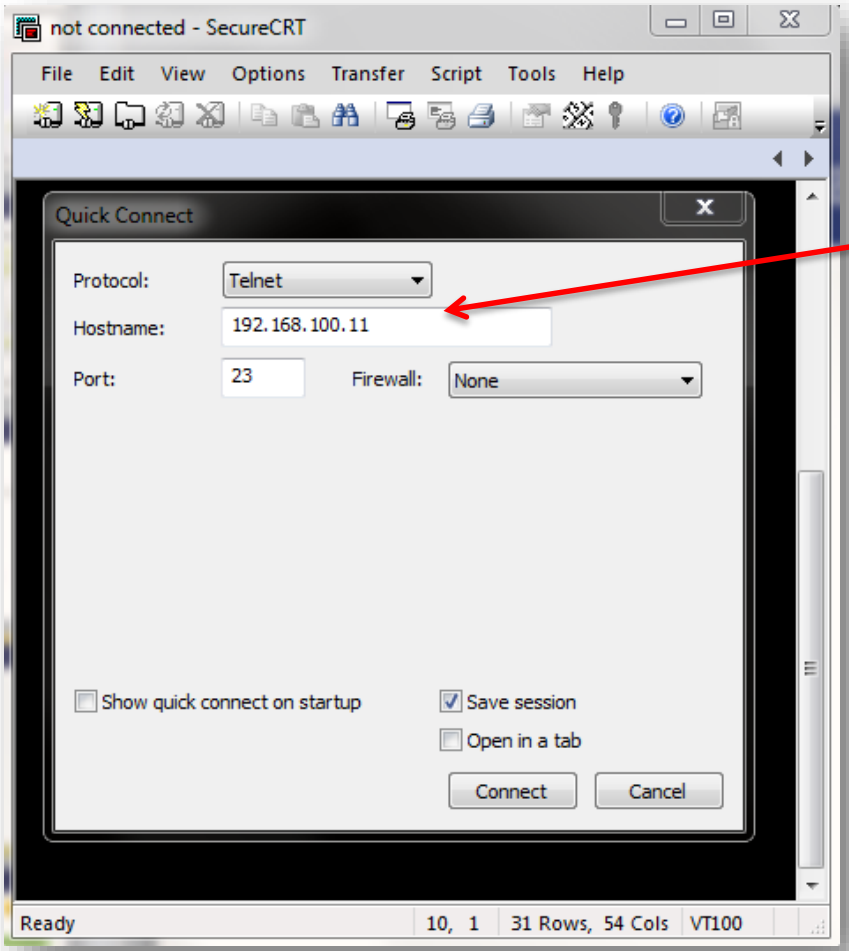
PLEASE NOTE!

- You will need to have Wireshark installed on your PC
- Downloadable URL: http://www.wireshark.org/download.html.

- Wireshark: 1.10.2 Stable & Latest version

- WinPcap: 4.1.3 Stable & Latest version
  - Included in Wireshark installation image

2.3.2.2 Remote Packet Capture



First we will need to setup the APC

Steps to setup

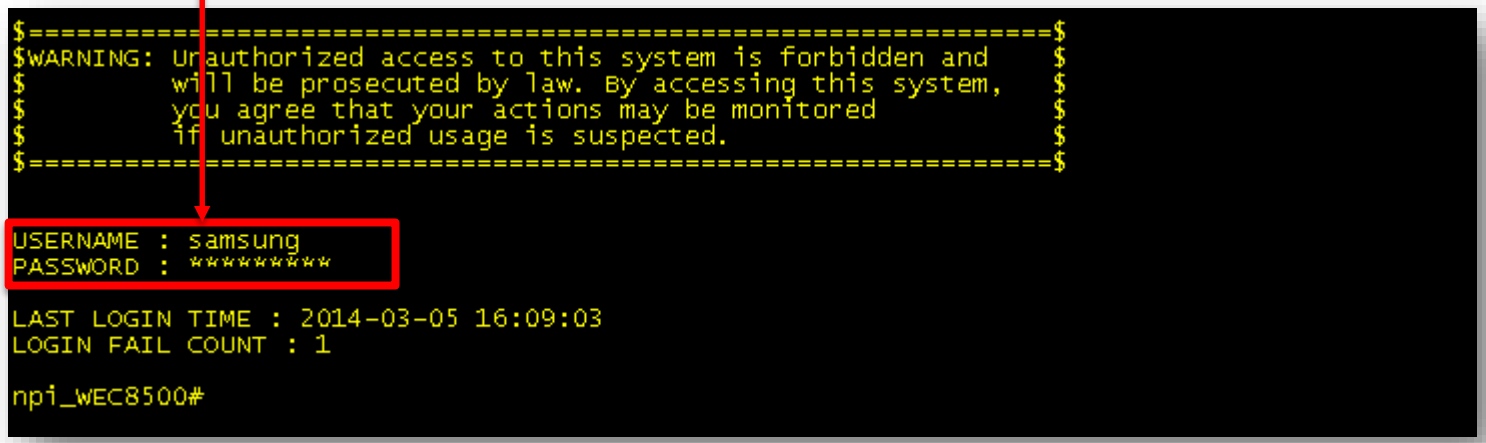
1. Start by telneting into the APC
2. Select the Operation Mode
3. Setup the pcap config for the station
4. Setup the pcap config for the AP
5. Enable the Filtering
6. Start the service
7. Setup our PC that has the Wireshark installed to capture the traffic

2.3.2.2 Remote Packet Capture

Samsung Wireless Enterprise™

Logging into the APC via CLI

Default User Name: samsung
Default Password: samsung



2.3.2.2 Select Operation Mode

Samsung Wireless Enterprise™

Using the show command we can view the current pcap config detail

```
npi_WEC8500# show pcap current-config detail

 - Current Status    : Idle
 - Filtering Target  : Station
 - Operation Mode    : Admin File Save(active mode)
 - Save Mode         : Local Disk
 - CAPWAP Option     : Disabled
 - Trigger Values    : Period(3600 secs)/File Size(104857600 bytes)/Packet Count(4000000 packets)

 - File Save Information(Local save mode)
       Local Path ..................................... /user/log/se/pcap/
       Disk Usage ..................................... 1280KB/204800KB(0.00%)
       Saved File List(Last 10)
         | File Name                                                | Uploaded | Status                | Time
         |
         | apc_T03-04-10-46-36_RAB.pcap                             |      100 |            Completed |  03-04
 11:04:10 |

       Total File Saved Count ......................... 1
       Error Count .................................... 0

 - Configured AP's MAC List
  No.       MAC Addr.          Filtering          Matched Count              Inbound Rate          Outbound Rate
 ===== ================== ========== ============================== ==================== ====================
=
 (empty)

 - Configured Station's MAC List
  No.       MAC Addr.          Filtering          Matched Count              Inbound Rate          Outbound Rate
 ===== ================== ========== ============================== ==================== ====================
=
 (empty)
```

2.3.2.2 Select Operation Mode

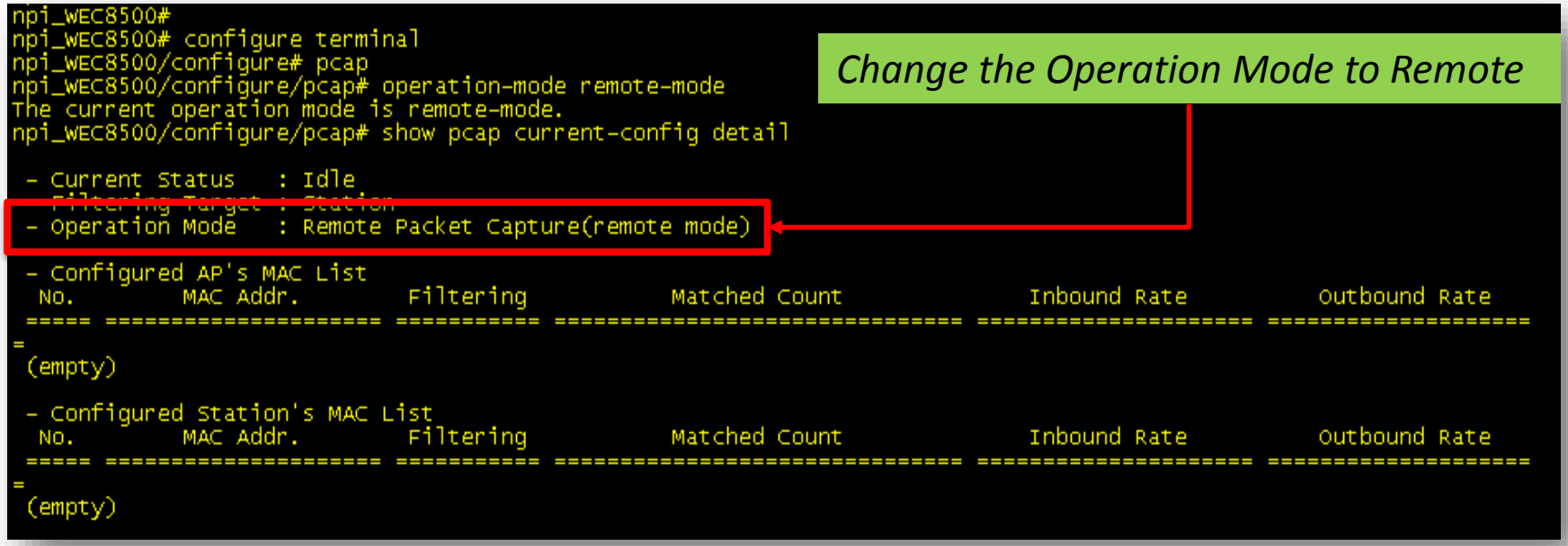
Samsung Wireless Enterprise™

```
npi_WEC8500# show pcap current-config detail

 - Current Status    : Idle
 - Filtering Target  : Station
 - Operation Mode    : Admin File Save(active mode)
 - Save Mode         : Local Disk
 - CAPWAP Option     : Disabled
 - Trigger Values    : Period(3600 secs)/File Size(104857600 bytes)/Packet Count(4000000 packets)

 - File Save Information(Local save mode)
       Local Path ..................................... /user/log/se/pcap/
       Disk Usage ..................................... 1280KB/204800KB(0.00%)
       Saved File List(Last 10)
         | File Name                                                | Uploaded | Status              | Time
         |
         | apc_T03-04-10-46-36_RAB.pcap                             |      100 |           Completed |  03-04
11:04:10 |

       Total File Saved Count ..... 1
       Error Count .....

 - Configured AP's MAC List
  No.       MAC Addr.       Filtering          Matched Count              Inbound Rate         Outbound Rate
 ===== ================== ========== ============================== ================== ==================
=
 (empty)

 - Configured Station's MAC List
  No.       MAC Addr.       Filtering          Matched Count              Inbound Rate         Outbound Rate
 ===== ================== ========== ============================== ================== ==================
=
 (empty)
```

Check the current operation mode

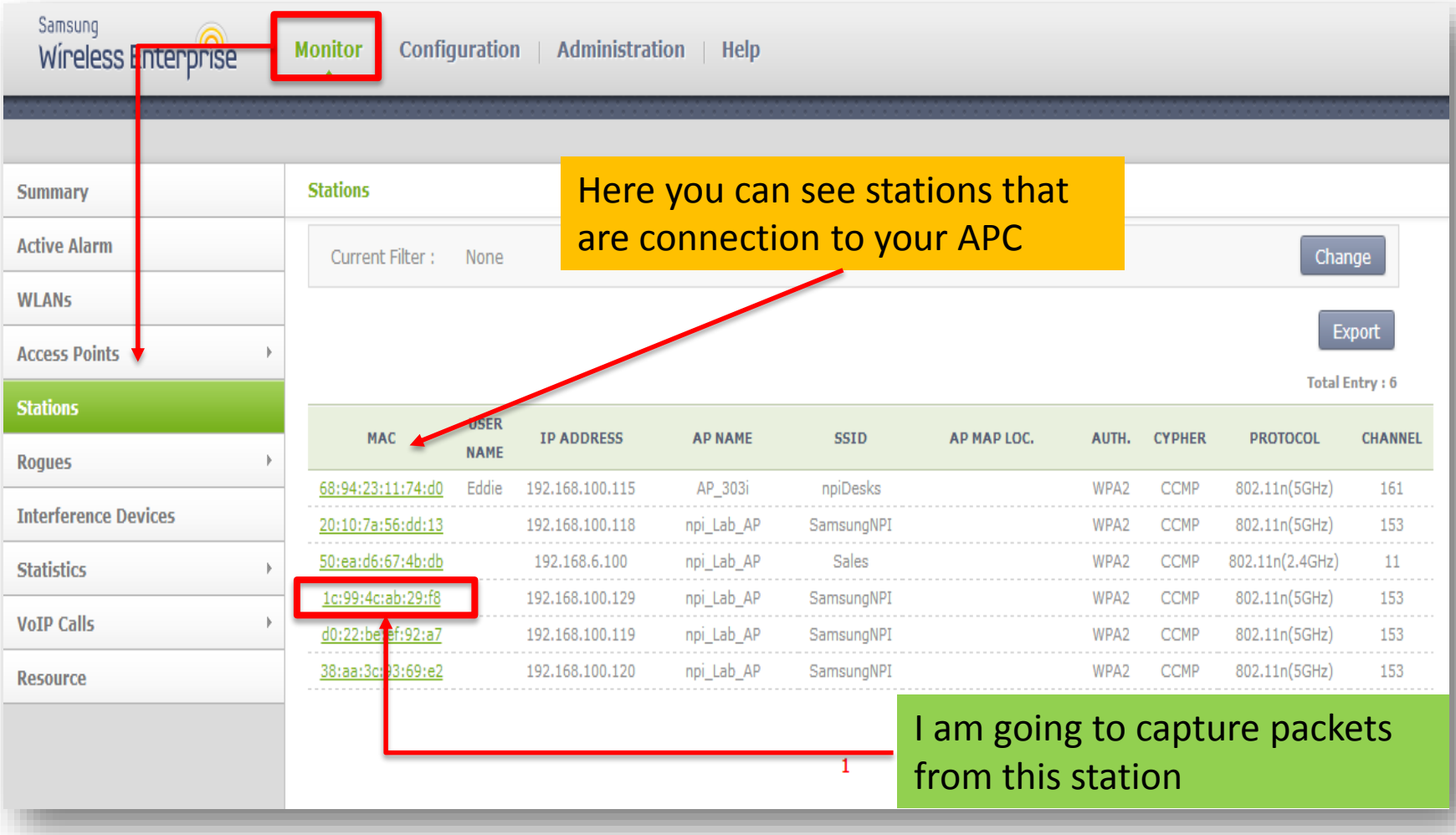
2.3.2.2 Select Operation Mode

Samsung Wireless Enterprise™



npi_WEC8500# configure terminal
npi_WEC8500/configure# pcap
npi_WEC8500/configure/pcap# operation-mode remote-mode

2.3.2.2 Configuring MAC of a station



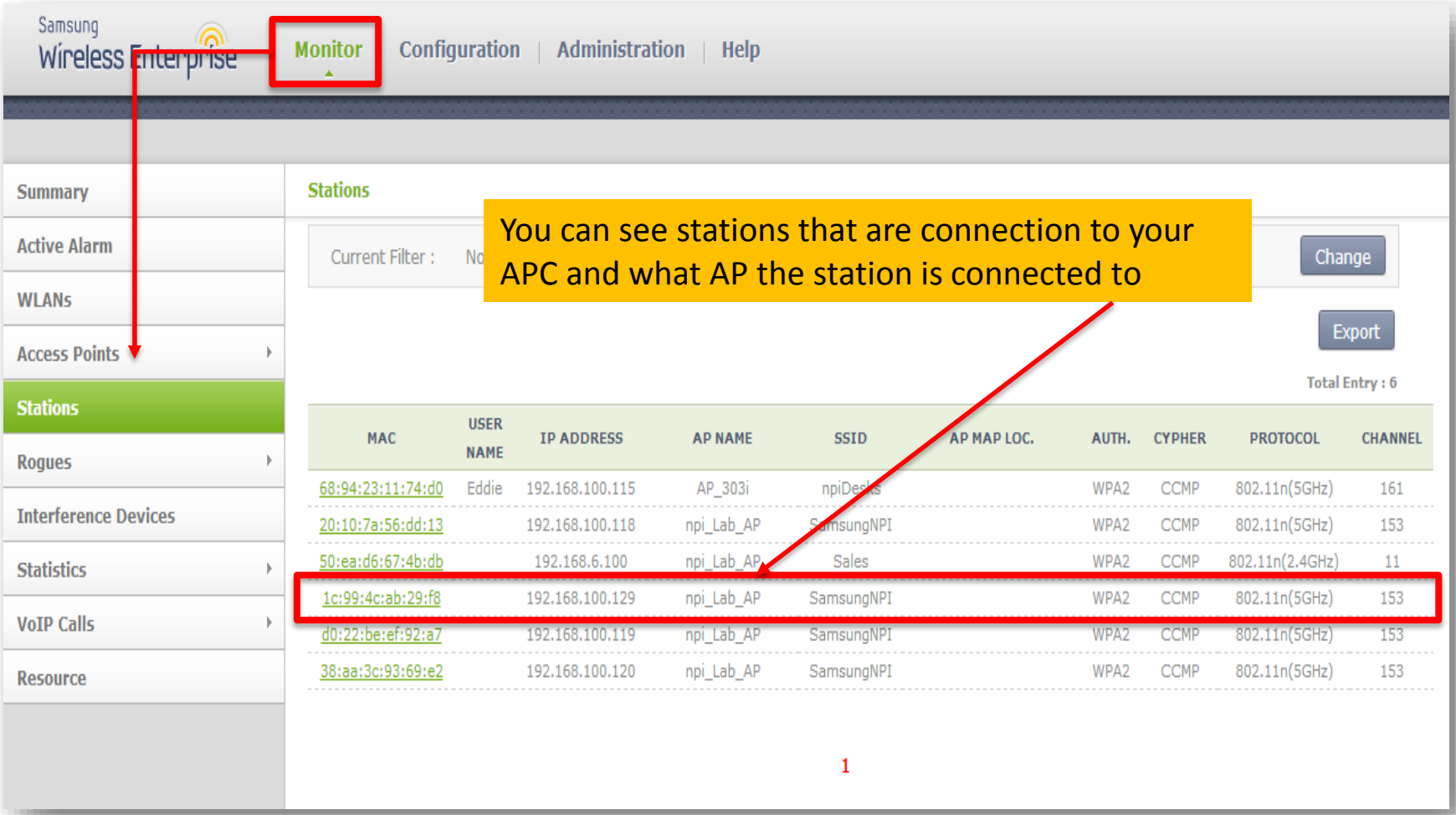
2.3.2.2 Configuring MAC of a station

Samsung Wireless Enterprise™

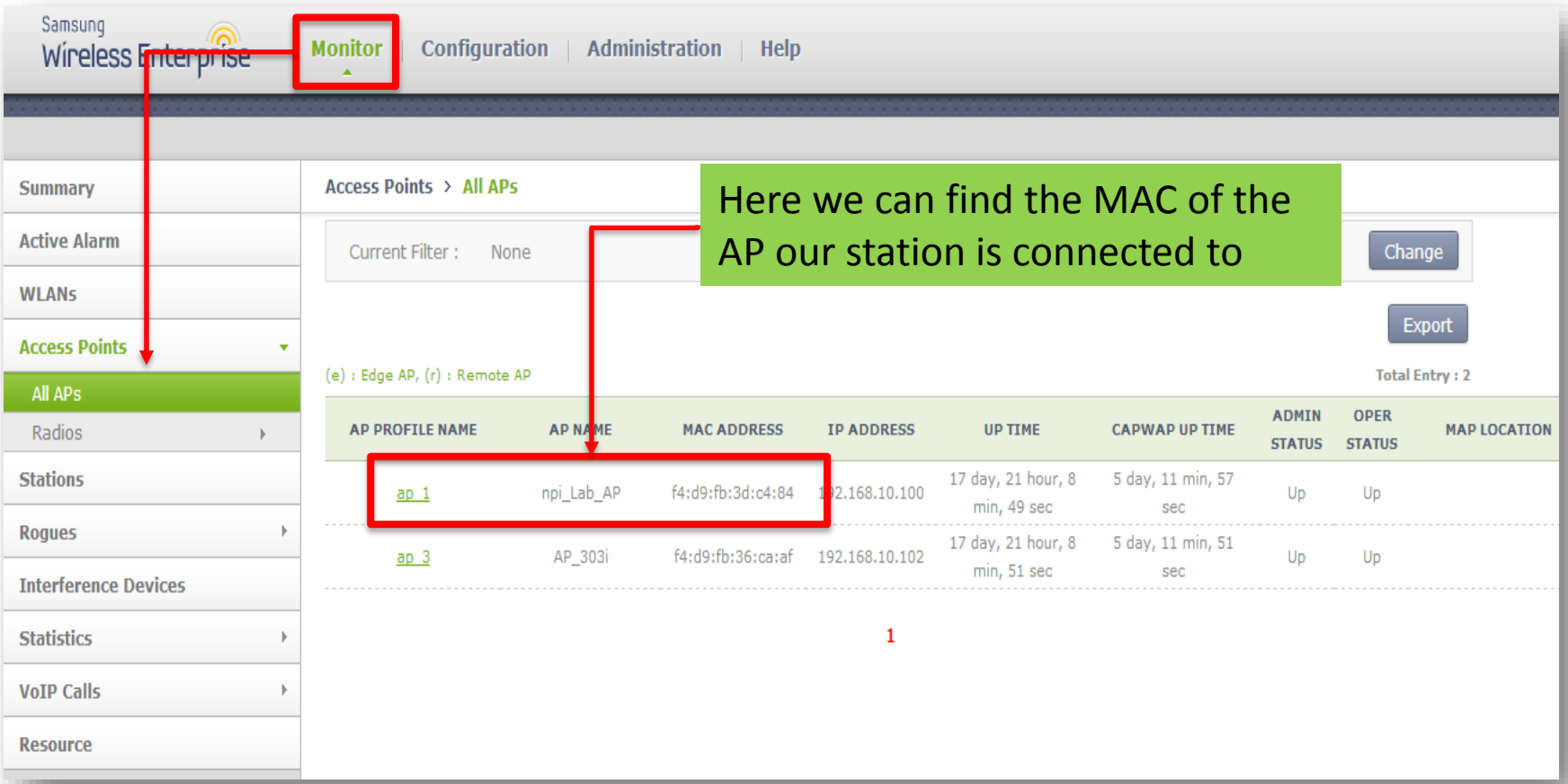
```
npi_WEC8500/configure/pcap# config-filter
npi_WEC8500/configure/pcap/config-filter# station-mac 1c:99:4c:ab:29:f8
The MAC value is added successfully.
npi_WEC8500/configure/pcap/config-filter# show pcap current-config detail

 - Current Status    : Idle
 - Filtering Target  : Station
 - Operation Mode    : Remote Packet Capture(remote mode)

 - Configured AP's MAC List
  No.        MAC Addr.        Filtering          Matched Count             Inbound Rate         Outbound Rate
 ===== ================== ========== ============================== ==================== ====================
 (empty)

 - Configured Station's MAC List
  No.        MAC Addr.        Filtering          Matched Count             Inbound Rate         Outbound Rate
 ===== ================== ========== ============================== ==================== ====================
    1   1C:99:4C:AB:29:F8   OFF<-------                           0              0.0 kbps             0.0 kbps
              AP   WN               SSID                      IPv4 Addr
             ---- ---- ------------------------------ ---------------
               1    1                     SamsungNPI 192.168.100.129
```

npi_WEC8500/configure/pcap# config-filter
npi_WEC8500/configure/pcap/config-filter# station-mac 1c:99:4c:ab:29:f8
npi_WEC8500/configure/pcap/config-filter# show pcap current-config detail

2.3.2.2 Configuring MAC of a station

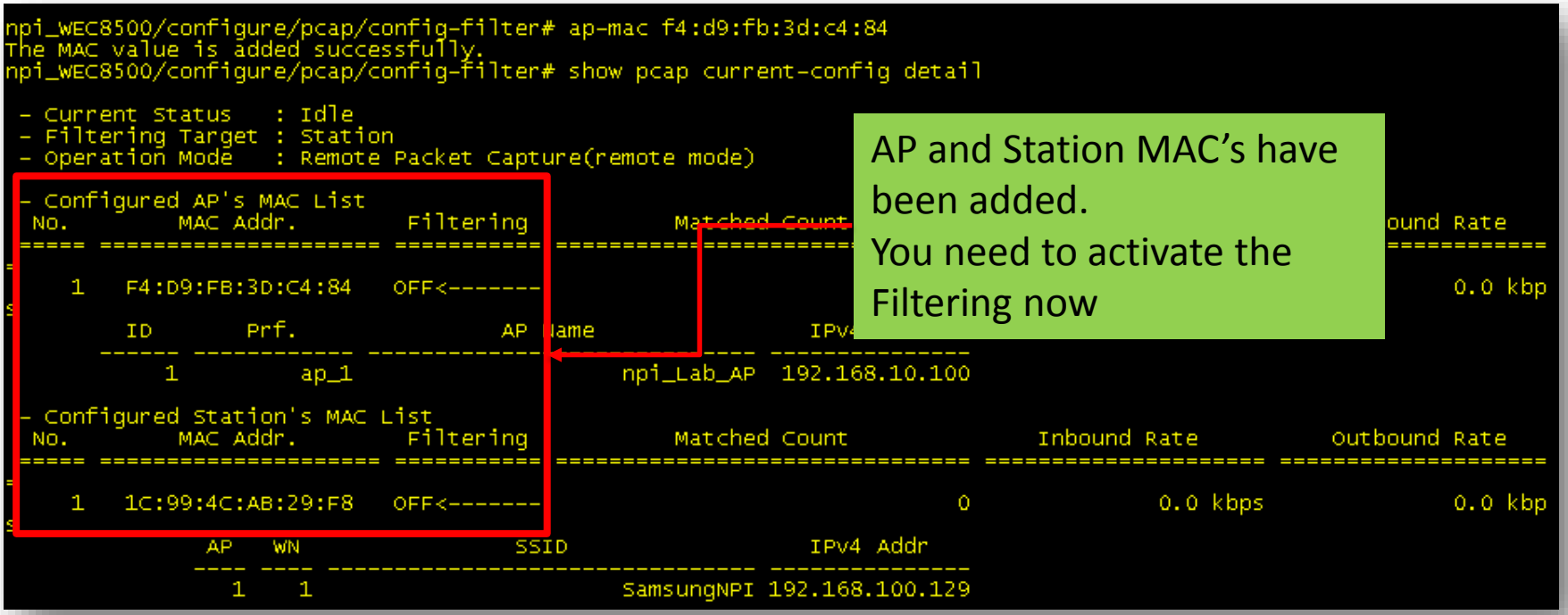


2.3.2.2 Configuring AP MAC address



2.3.2.2 Configuring AP MAC address

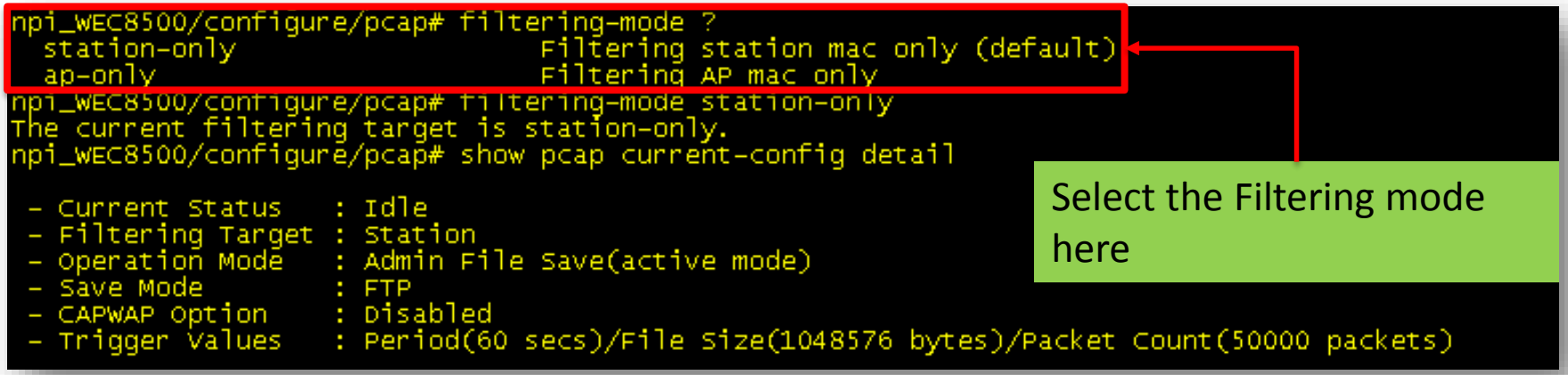
Samsung Wireless Enterprise™



npi_WEC8500/configure/pcap/config-filter# ap-mac f4:d9:fb:3d:c4:84
npi_WEC8500/configure/pcap/config-filter# show pcap current-config detail

2.3.2.2 Configuring Filtering Mode

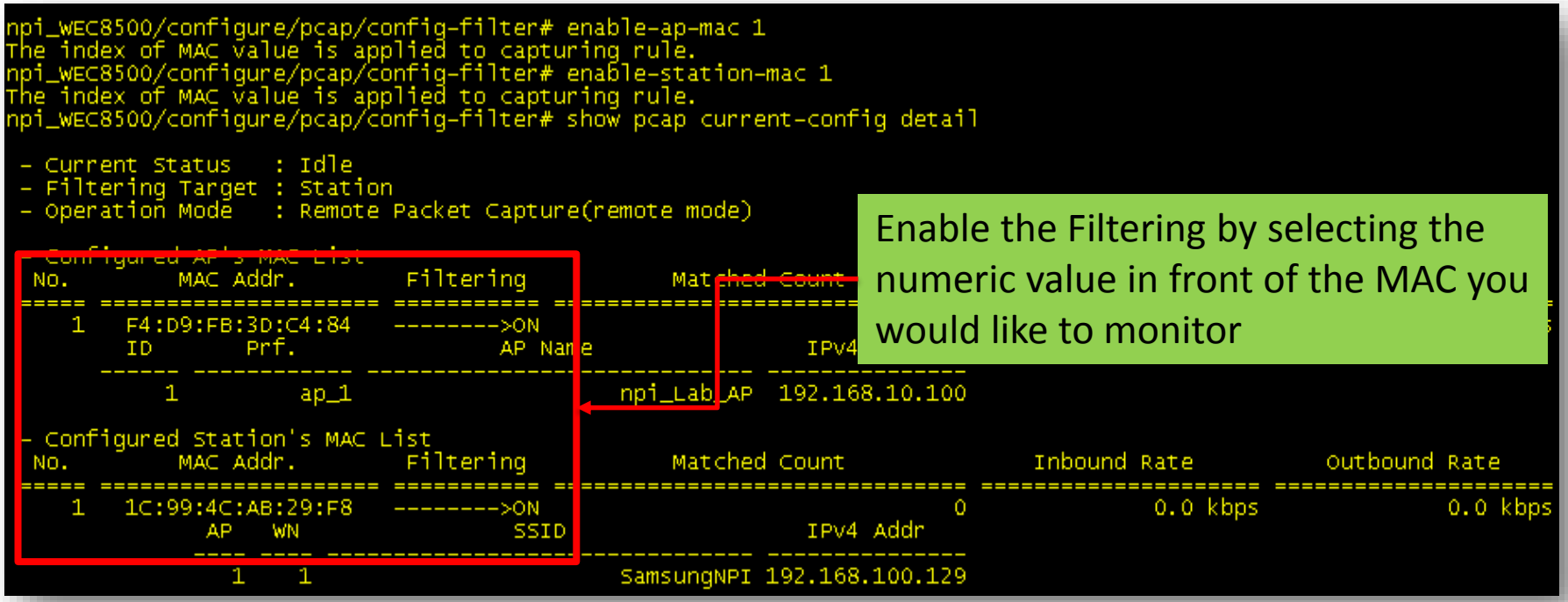
Samsung Wireless Enterprise™



npi_WEC8500/configure/pcap# filtering-mode ?
station-only Filtering station mac only (default)
ap-only Filtering AP mac only
npi_WEC8500/configure/pcap# filtering-mode station-only
The current filtering target is station-only.
npi_WEC8500/configure/pcap# show pcap current-config detail

2.3.2.2 Configuring Filtering Mode

Samsung Wireless Enterprise™




```
npi_WEC8500/configure/pcap/config-filter# enable-ap-mac 1
The index of MAC value is applied to capturing rule.
npi_WEC8500/configure/pcap/config-filter# enable-station-mac 1
The index of MAC value is applied to capturing rule.
npi_WEC8500/configure/pcap/config-filter# show pcap current-config detail
```

2.3.2.2 Starting the Service

Samsung Wireless Enterprise™

```
npi_WEC8500/configure/pcap/config-filter# exit
npi_WEC8500/configure/pcap# start-service
Service is started successfully.
npi_WEC8500/configure/pcap# show pcap current-config detail

- Current Status    : Wating for client's access
- Filtering Target  : Station
- Operation Mode    : Remote Packet Capture(remote mode)

- Configured AP's MAC List
 No.        MAC Addr.        Filtering          Matched Count            Inbound Rate         Outbound Rate
===== ================== ========== ============================== ==================== ====================
    1   F4:D9:FB:3D:C4:84   -------->ON                                0              0.0 kbps             0.0 kbps
        ID       Prf.              AP Name                IPv4 Addr
      ------ ------------ ---------------------------- ---------------
           1         ap_1                   npi_Lab_AP  192.168.10.100

- Configured Station's MAC List
 No.        MAC Addr.        Filtering          Matched Count            Inbound Rate         Outbound Rate
===== ================== ========== ============================== ==================== ====================
    1   1C:99:4C:AB:29:F8   -------->ON                                0              0.0 kbps             0.0 kbps
             AP   WN               SSID                    IPv4 Addr
            ---- ---- -------------------------------- ---------------
              1    1                      SamsungNPI 192.168.100.129
```

The APC is now waiting for Wireshark to make the remote connection

npi_WEC8500/configure/pcap/config-filter# exit
npi_WEC8500/configure/pcap# start-service
Service is started successfully.
npi_WEC8500/configure/pcap# show pcap current-config detail

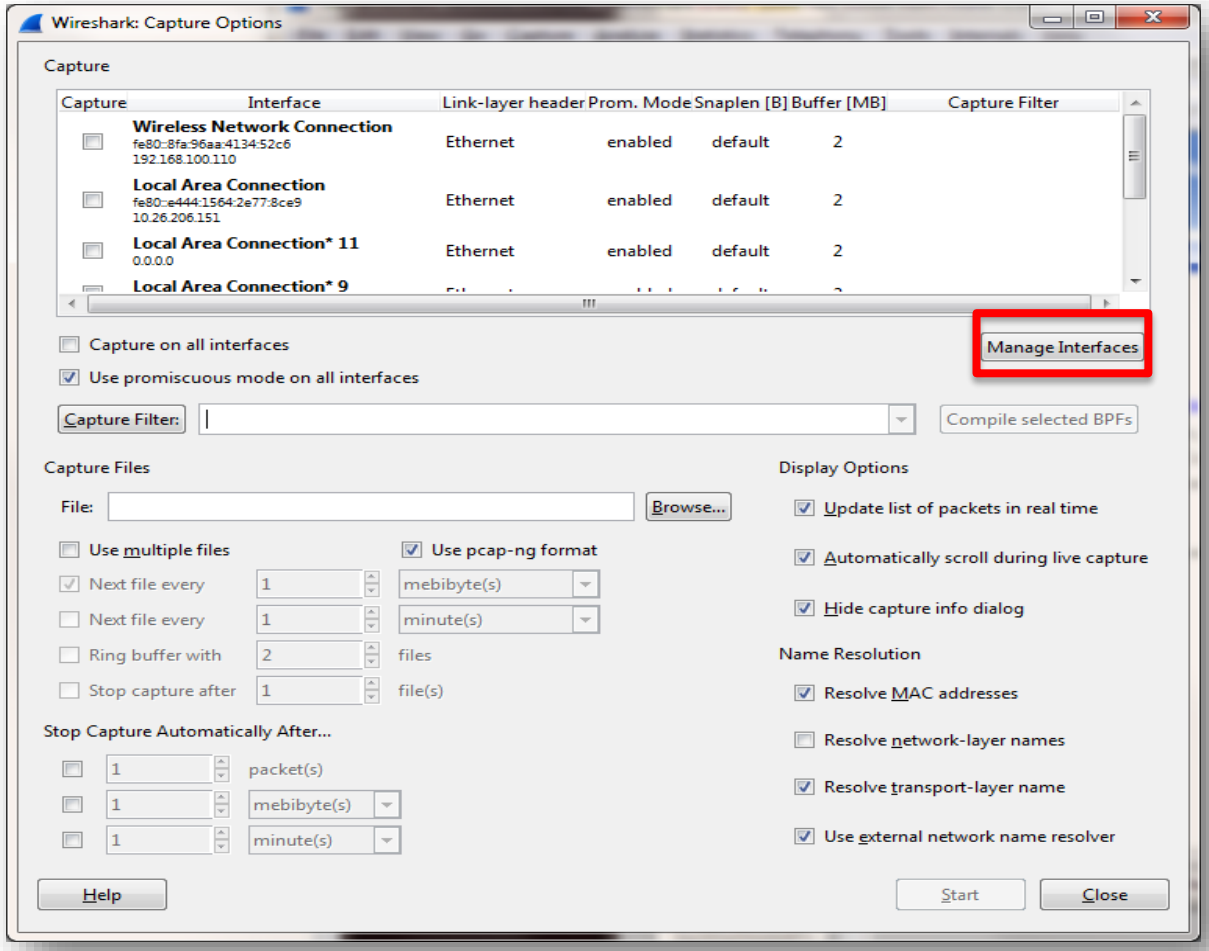
2.3.2.2 Computer Setup

The configuration for the capture of packets is finished, now we need to setup our Wireshark on our computer

2.3.2.2 Computer Setup

Samsung Wireless Enterprise™

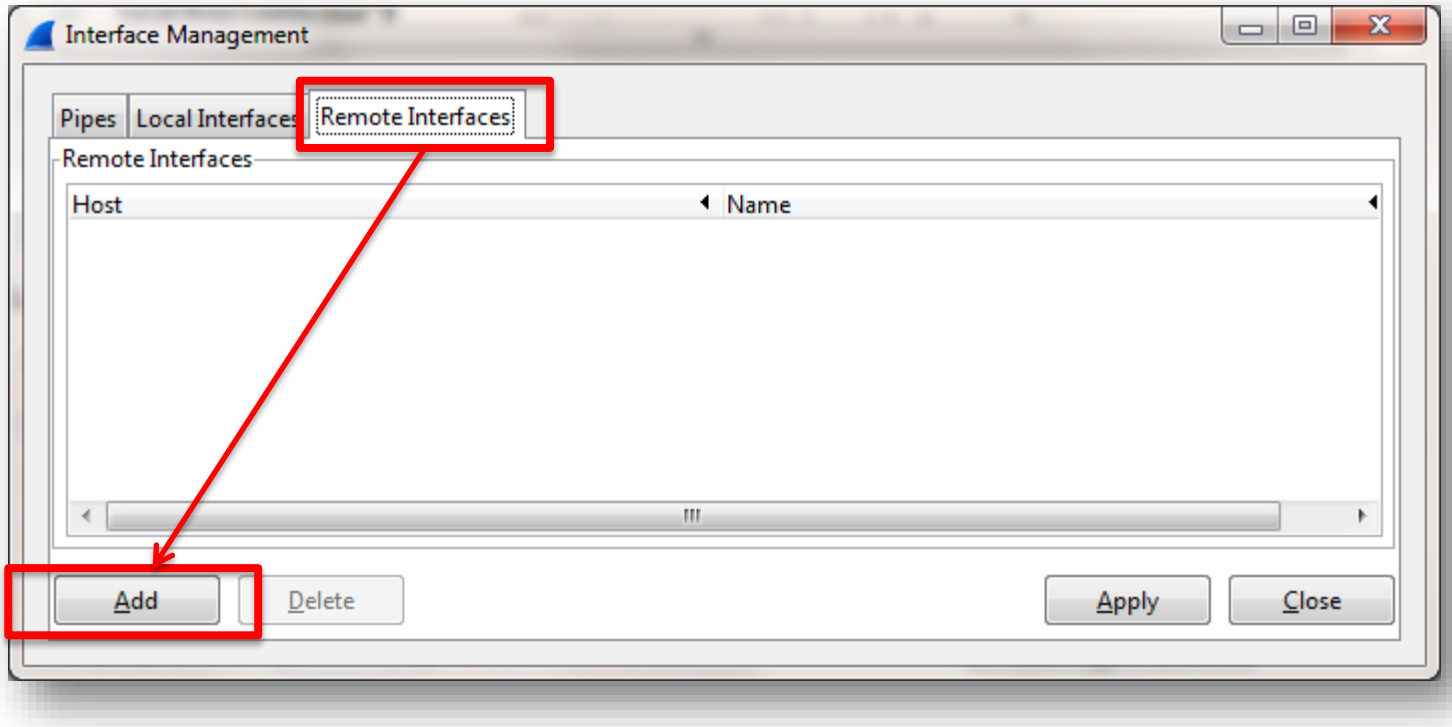
Capture → Options… ‘Manage Interfaces’ click



2.3.2.2 Computer Setup

Samsung Wireless Enterprise™

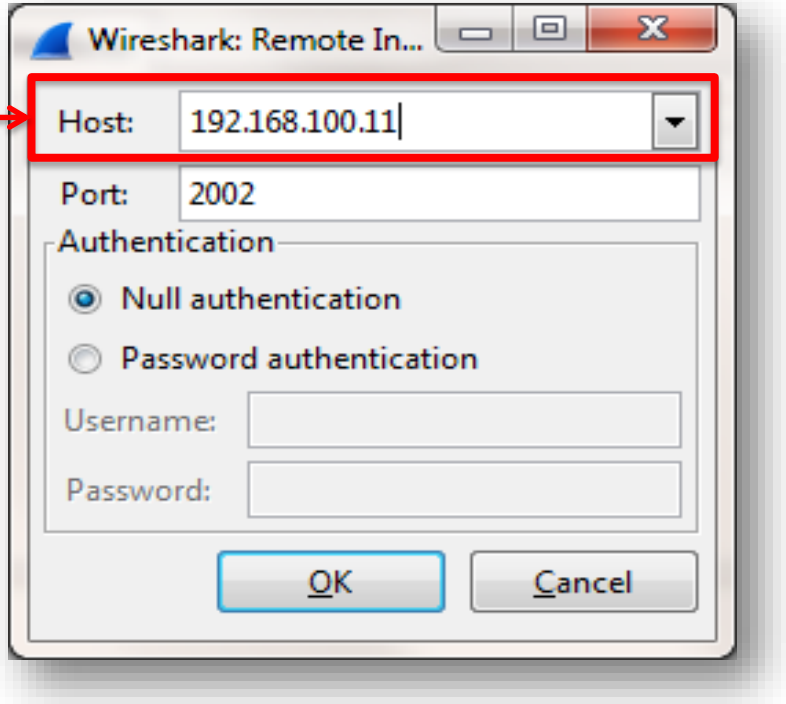
‘Remote Interfaces’ tab click and ‘Add’ Click



2.3.2.2 Computer Setup

Samsung Wireless Enterprise™

Insert APC IP address and Port (default 2002)
Authentication (Null)

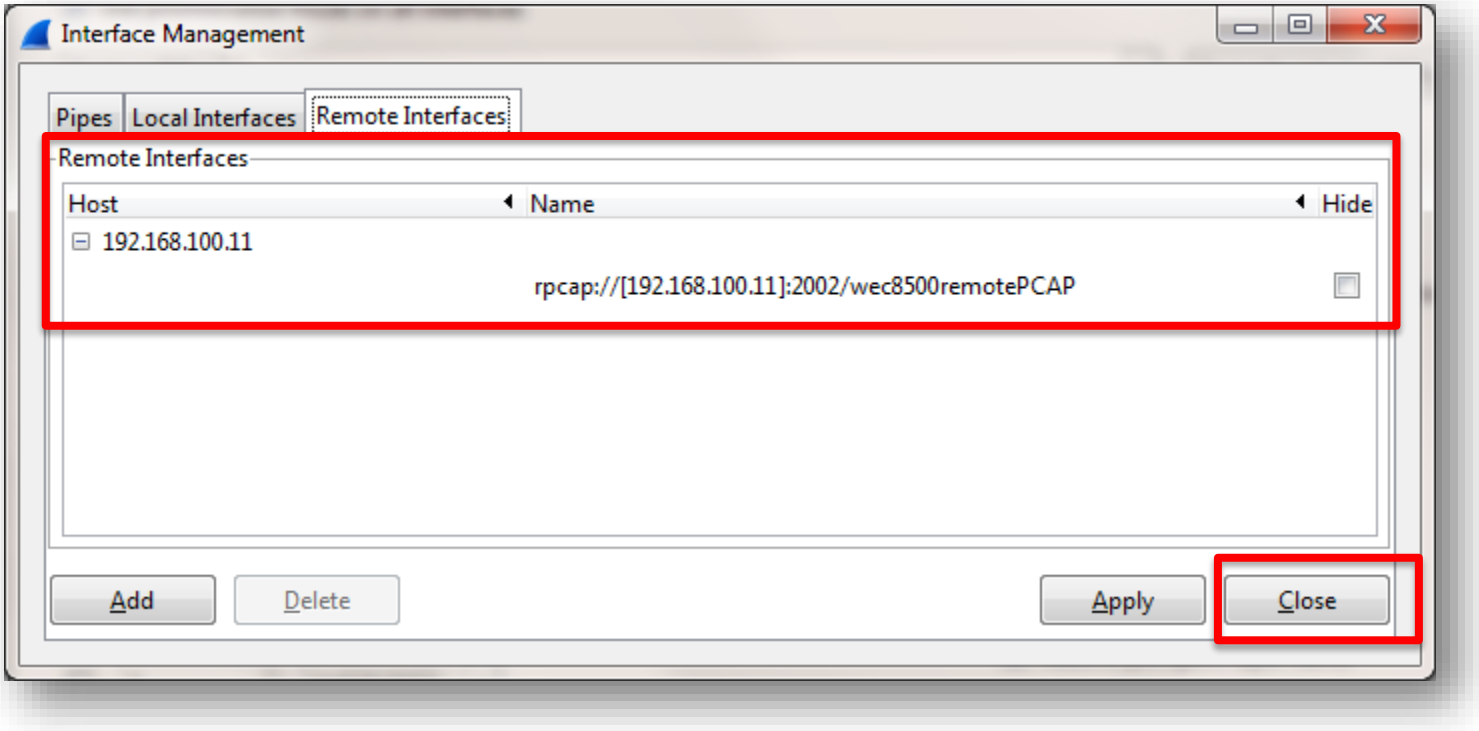


This address should be the Interface IP on the network that your PC is on

2.3.2.2 Computer Setup

Samsung Wireless Enterprise™

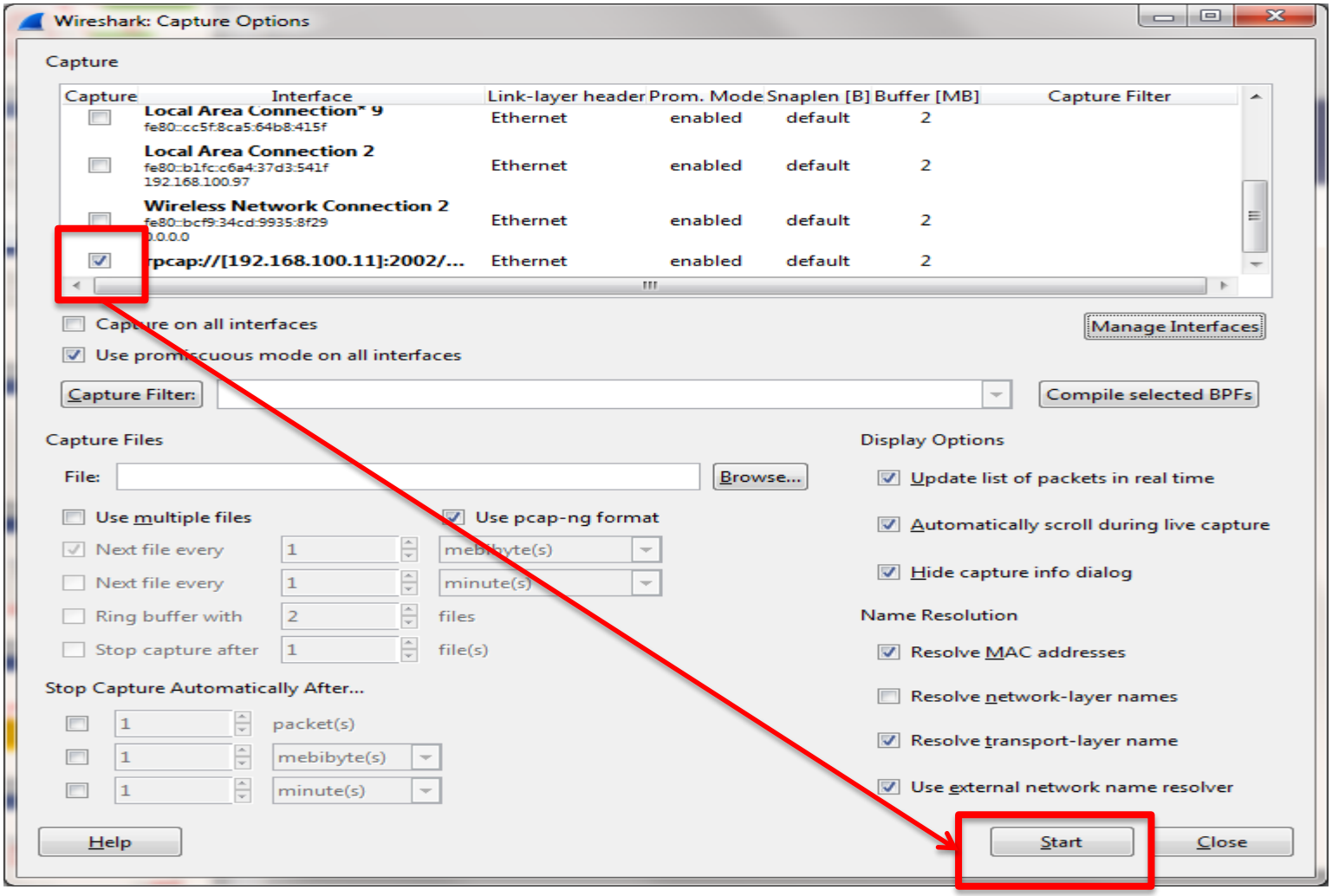
Check the registration of AP Controller, ‘Close’ click



2.3.2.2 Computer Setup

Samsung Wireless Enterprise™

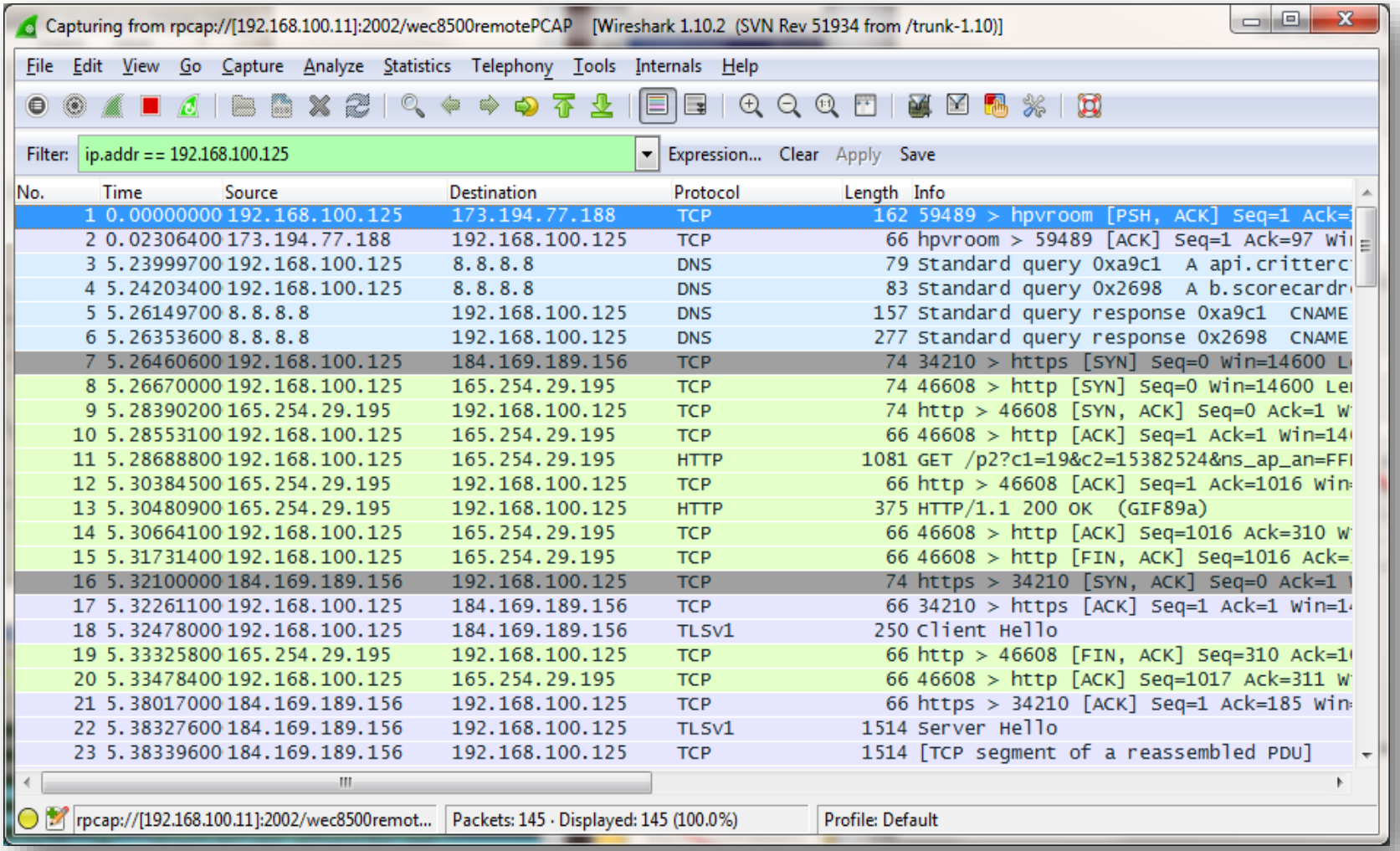
Select AP Controller Interface, ‘Start’ click



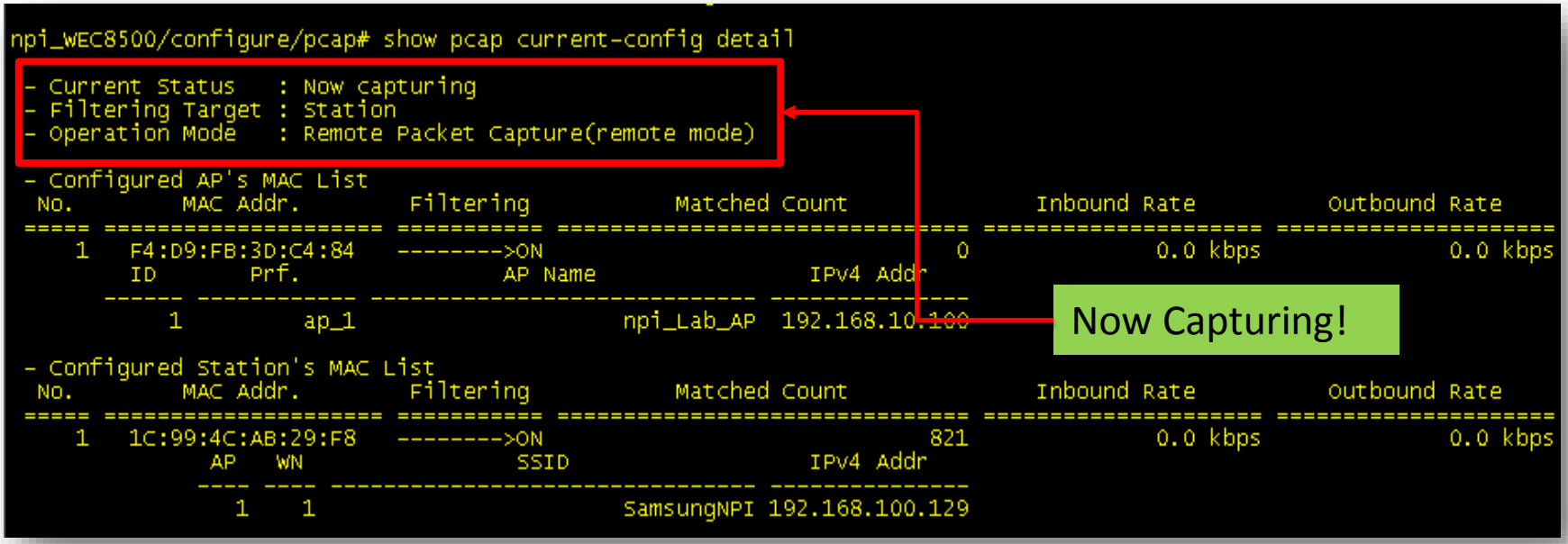
2.3.2.2 Computer Setup

Samsung Wireless Enterprise™

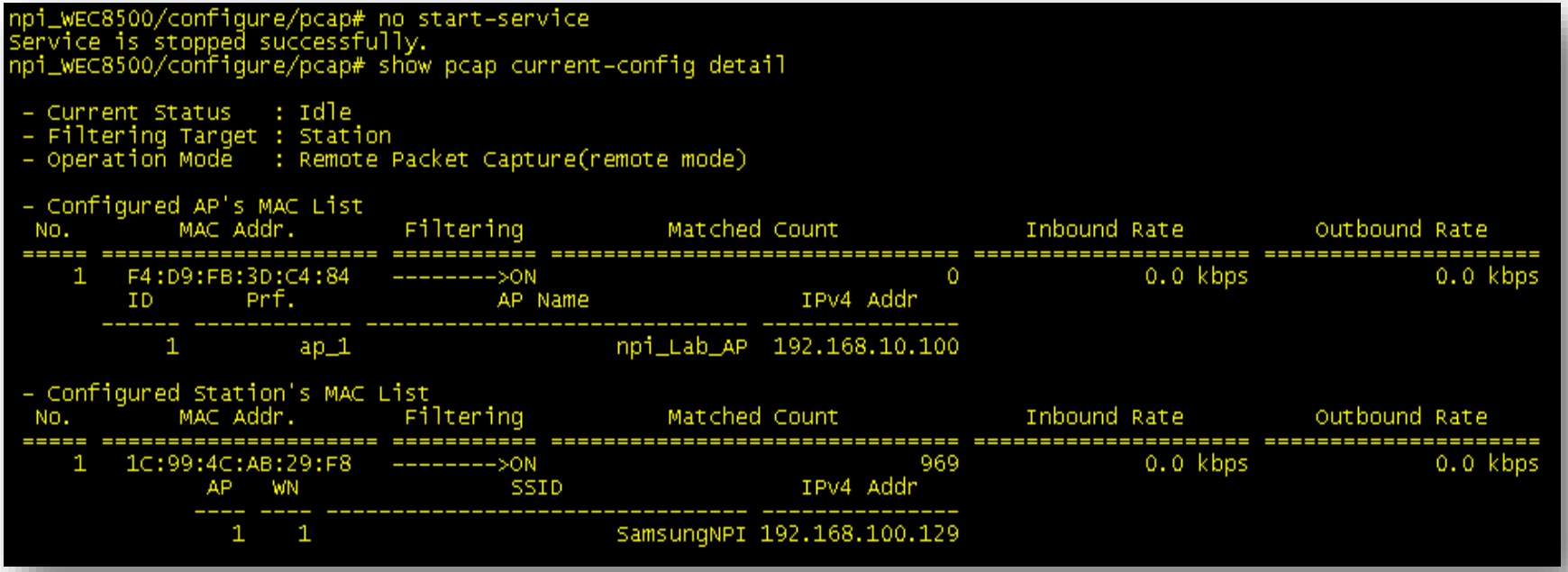
Display Capturing packets



2.3.2.2 Computer Setup



2.3.2.2 Stopping the Capture



npi_WEC8500/configure/pcap# no start-service
Service is stopped successfully.
npi_WEC8500/configure/pcap# show pcap current-config detail

2.3.2.2 Stopping the Capture

```
npi_WEC8500/configure/pcap/config-filter# no ap-mac f4:d9:fb:3d:c4:84
The MAC value is deleted successfully.
npi_WEC8500/configure/pcap/config-filter# no station-mac 1c:99:4c:ab:29:f8
The MAC value is deleted successfully.
There is no available MAC filtering value(station and AP), so the service will be stopped.
npi_WEC8500/configure/pcap/config-filter# show pcap current-config detail

 - Current Status    : Idle
 - Filtering Target  : Station
 - Operation Mode    : Remote Packet Capture(remote mode)

 - Configured AP's MAC List
  No.        MAC Addr.        Filtering          Matched Count             Inbound Rate         Outbound Rate
 ===== ==================== ========== ============================== ==================== ====================
 (empty)

 - Configured Station's MAC List
  No.        MAC Addr.        Filtering          Matched Count             Inbound Rate         Outbound Rate
 ===== ==================== ========== ============================== ==================== ====================
 (empty)
```

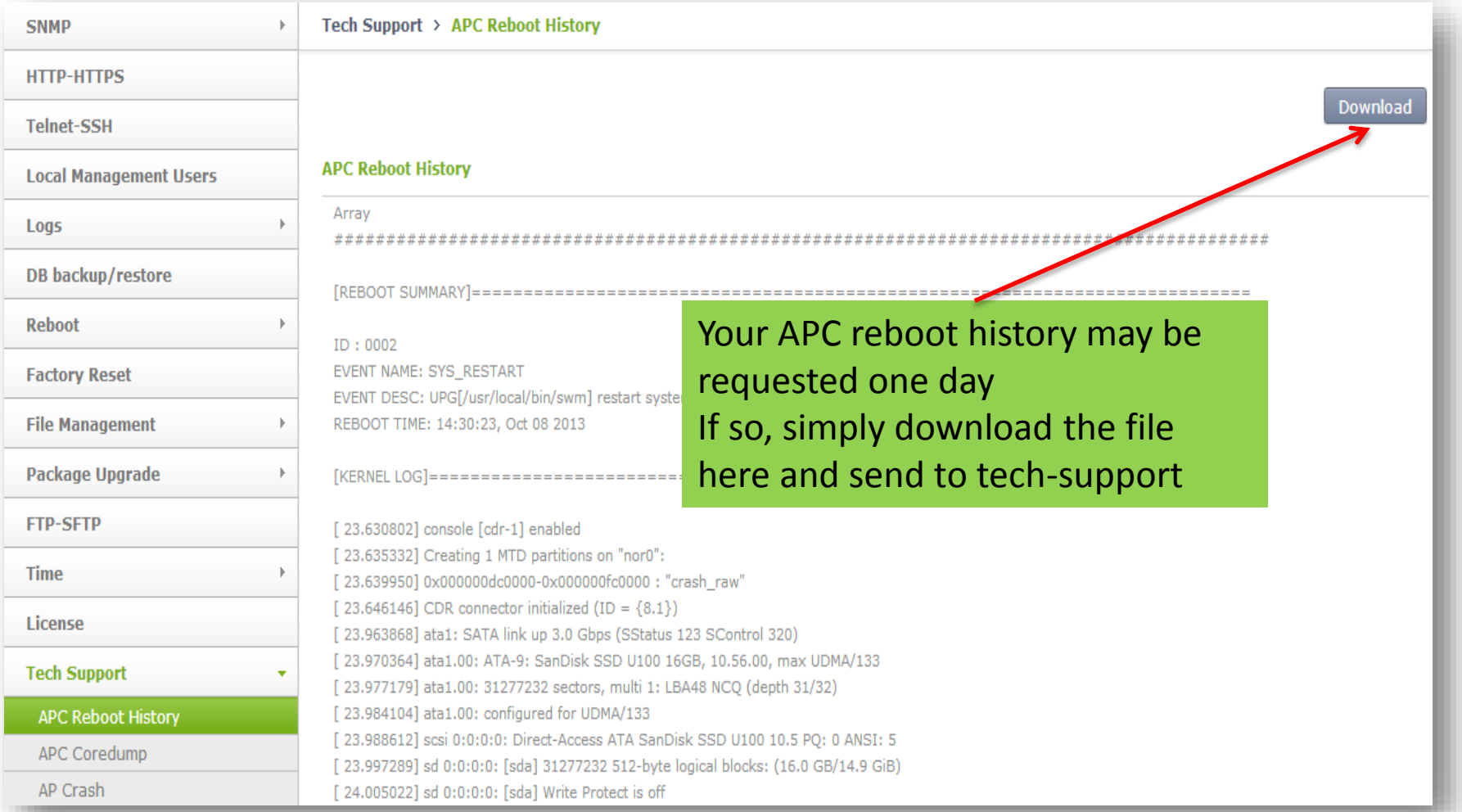
npi_WEC8500/configure/pcap/config-filter# no ap-mac f4:d9:fb:3d:c4:84
npi_WEC8500/configure/pcap/config-filter# no station-mac 1c:99:4c:ab:29:f8
There is no available MAC filtering value(station and AP), so the service will be stopped.
npi_WEC8500/configure/pcap/config-filter# show pcap current-config detail

Samsung Wireless Enterprise™

Tech Support

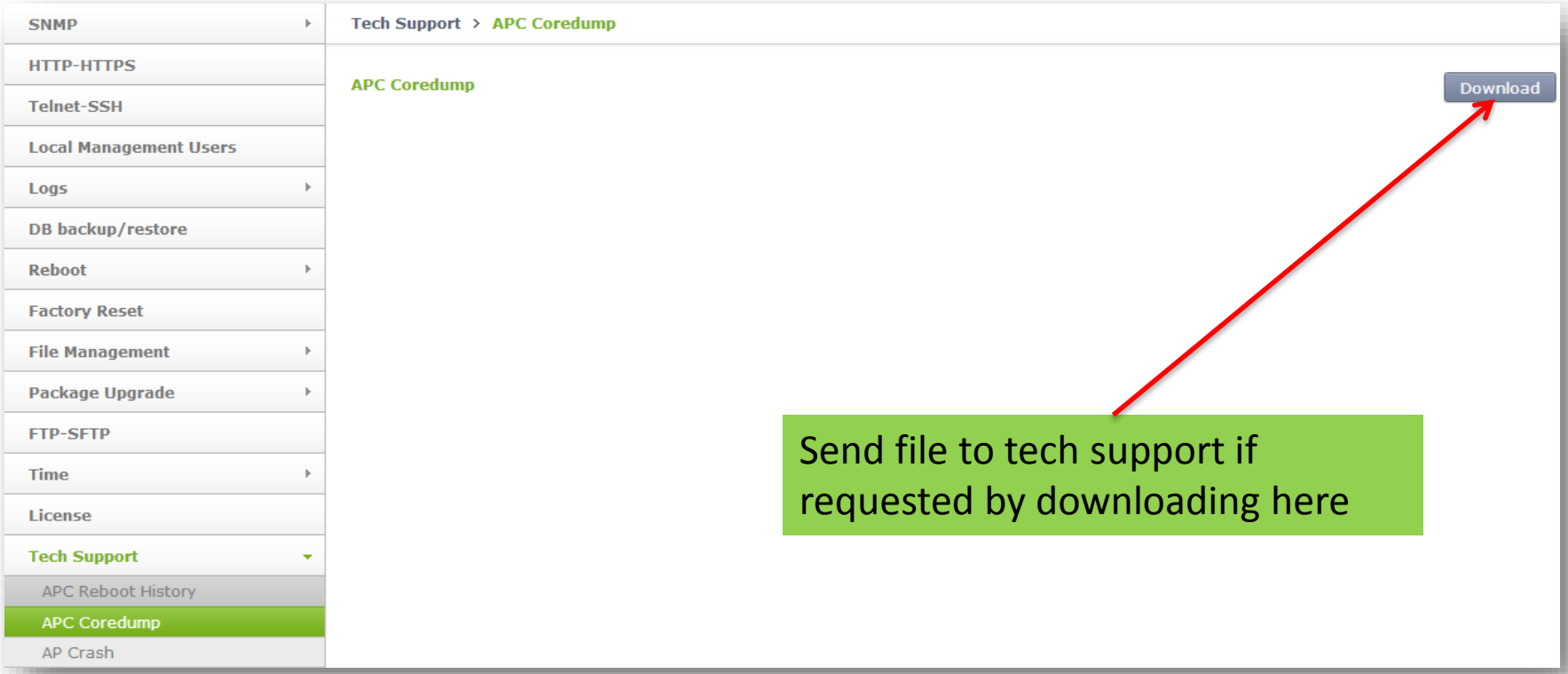
Samsung Wireless Enterprise™

APC Reboot History



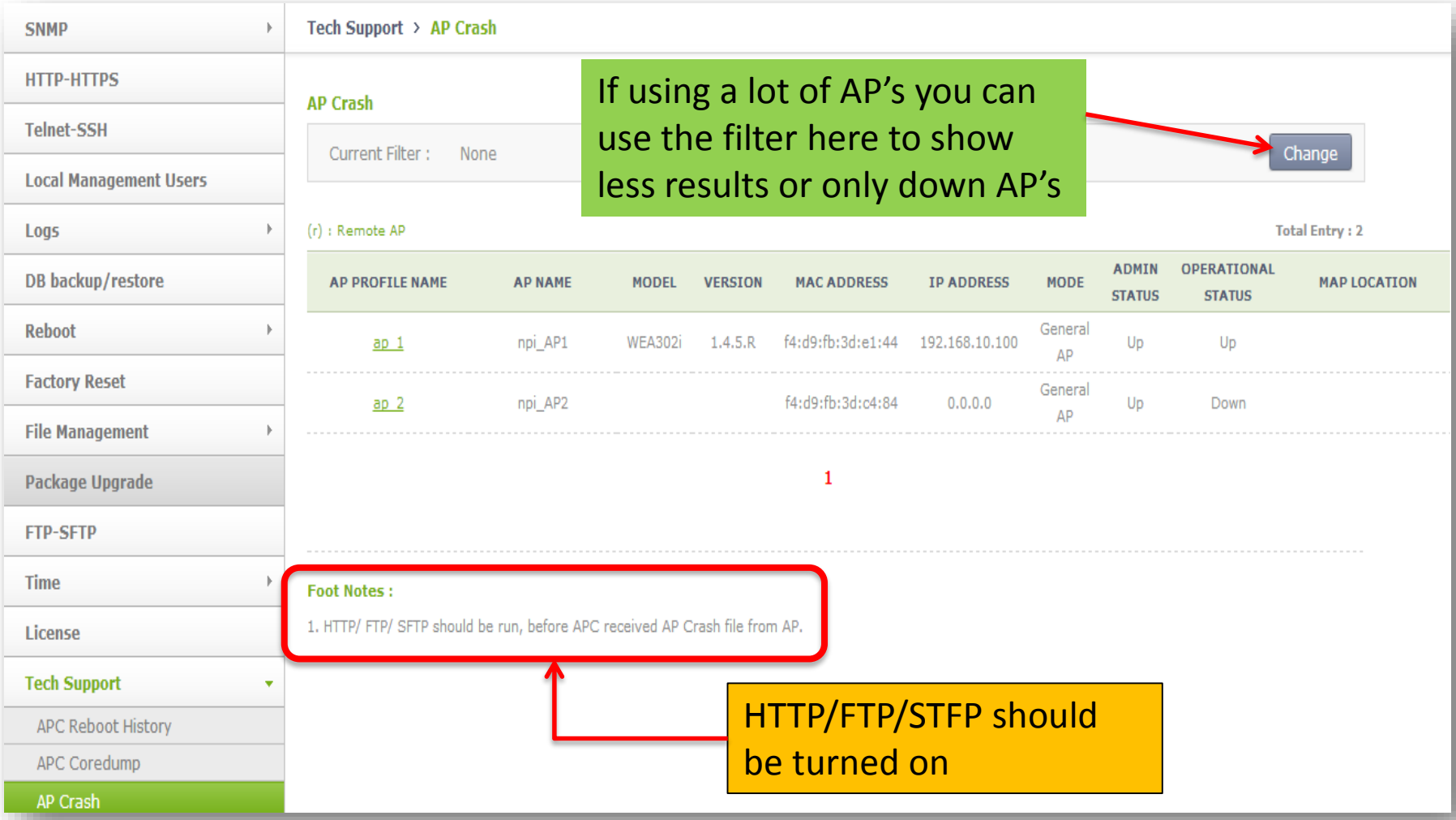
Samsung Wireless Enterprise™

APC Coredump



Samsung Wireless Enterprise™

AP Crash

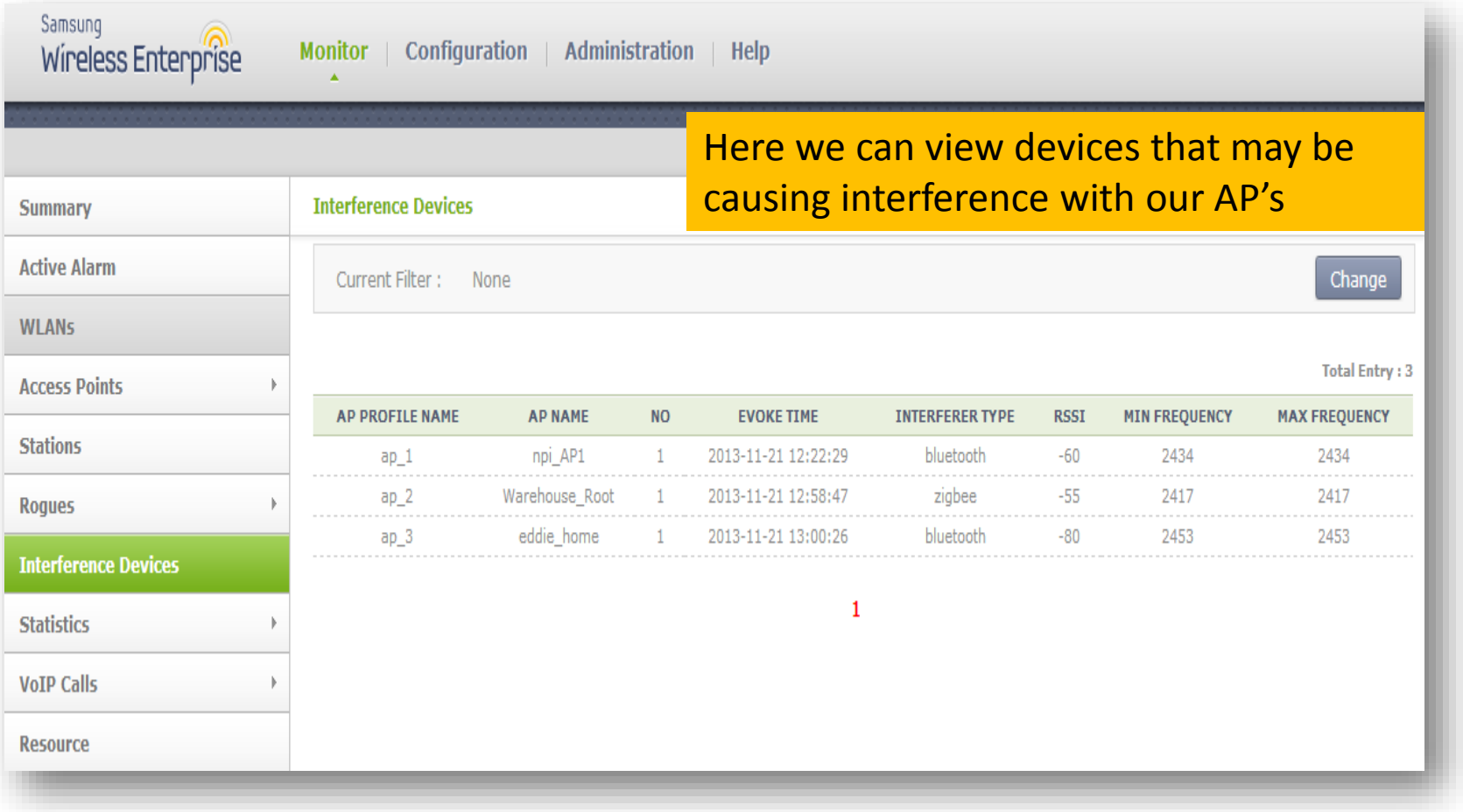


Lab 18 -

Download the APC Reboot and Coredump Files

1. Go to Administration → Tech Support
2. Go to APC Reboot History → Download file
3. Go to APC Coredump → Download file

2.5 Interference Devices



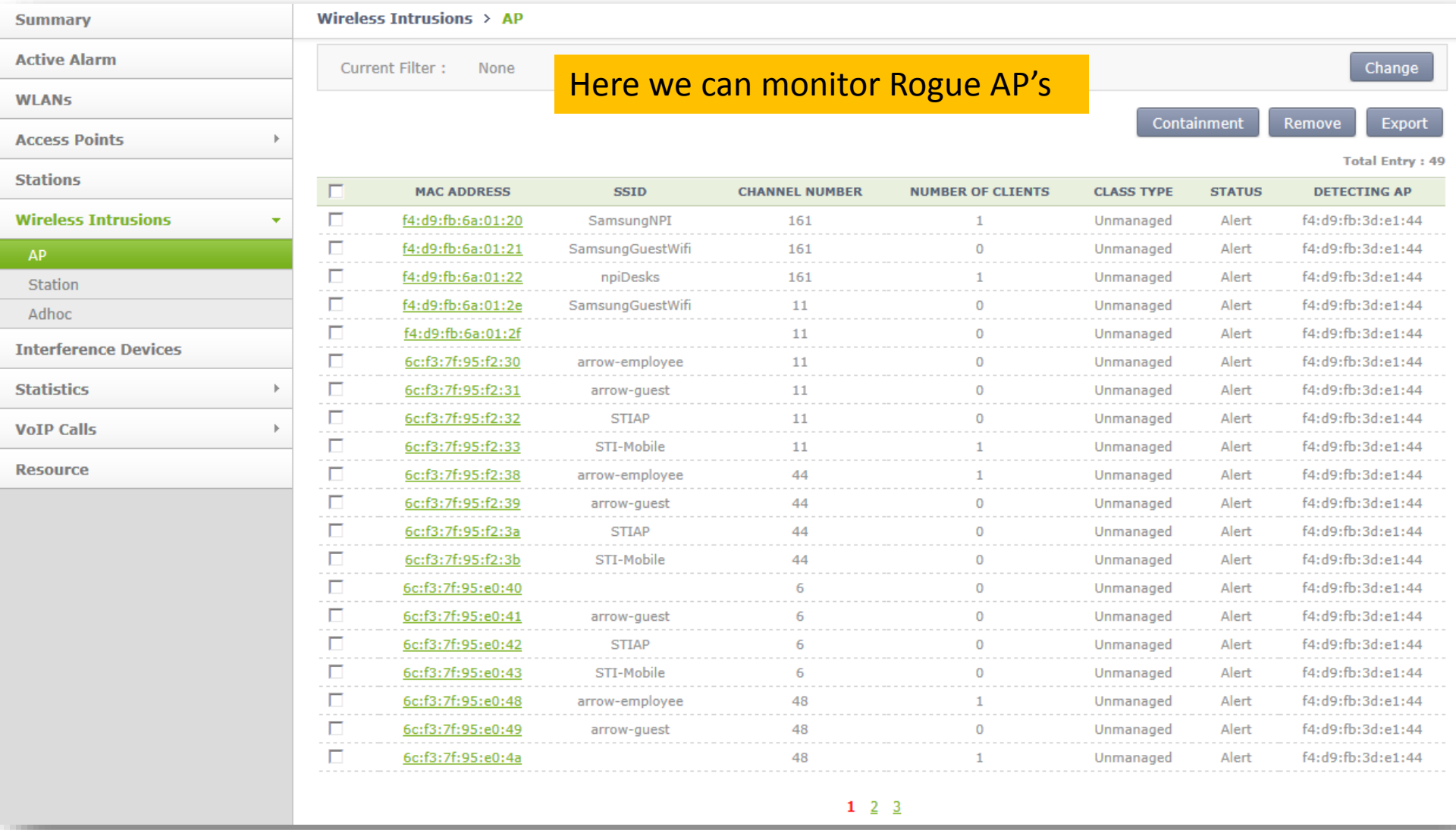
Samsung Wireless Enterprise™

2.6 Rogue AP's and Stations

- 2.6.1 Monitoring Rogue
- 2.6.2 Setup White/Black List

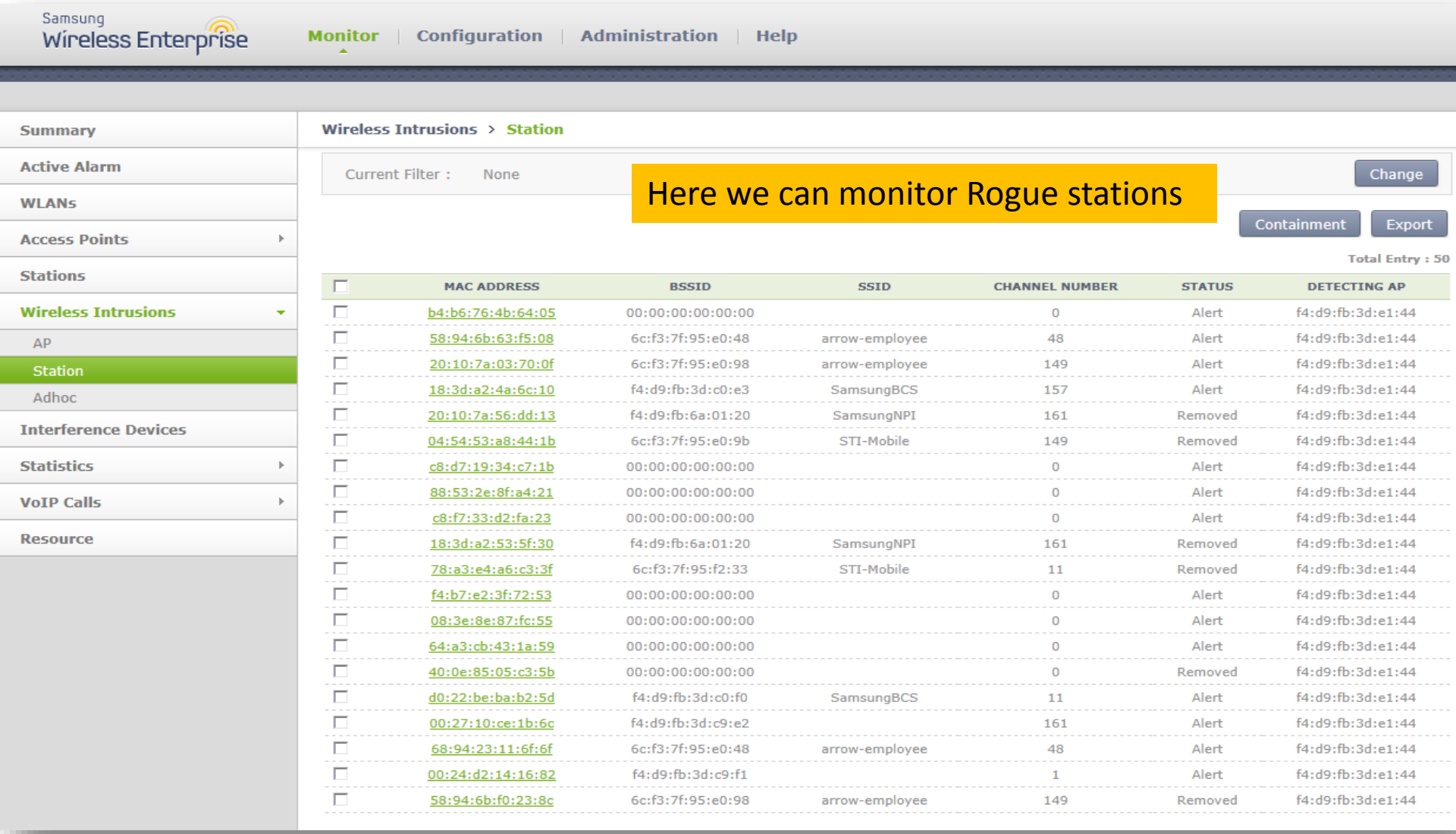
2.6.1 Monitoring Rogue

Samsung Wireless Enterprise™



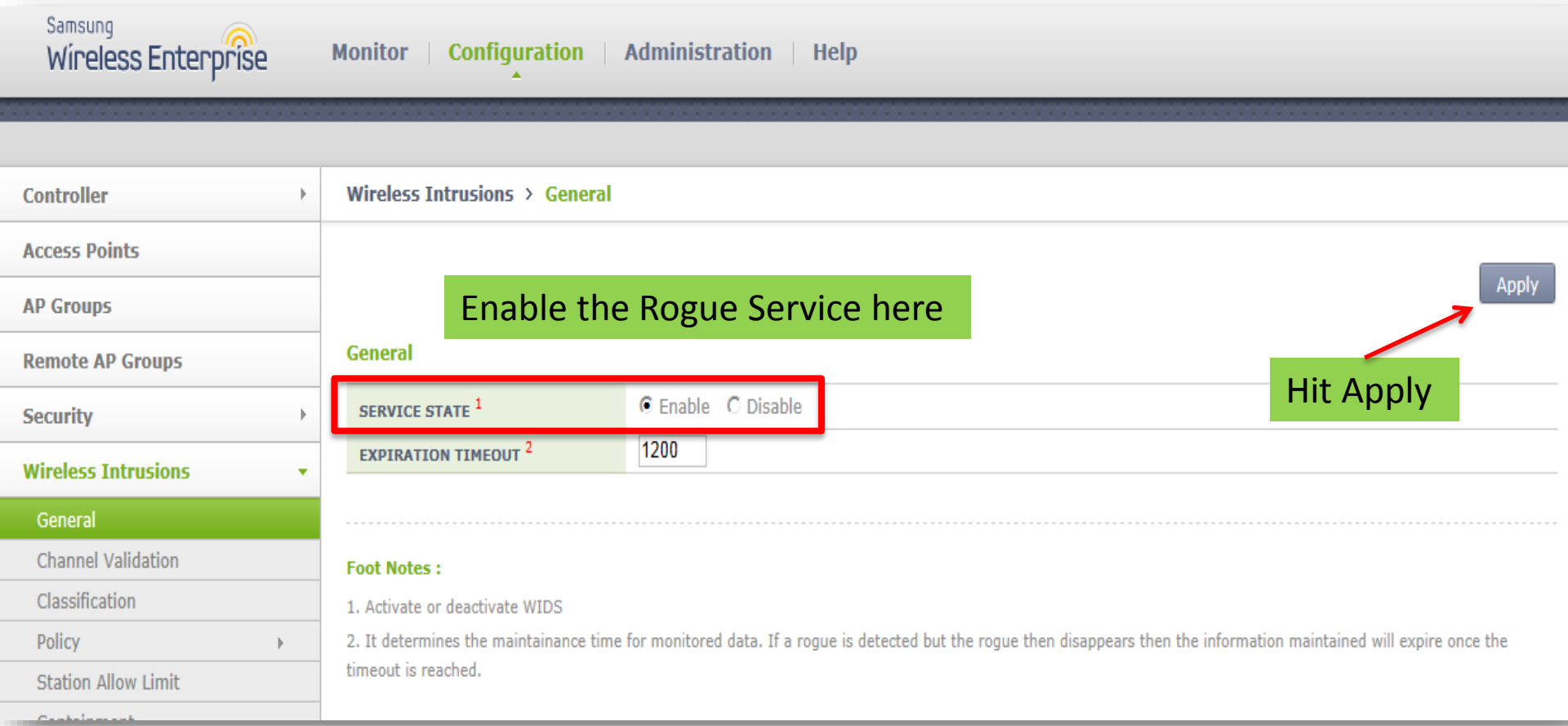
2.6.1 Monitoring Rogue

Samsung Wireless Enterprise™

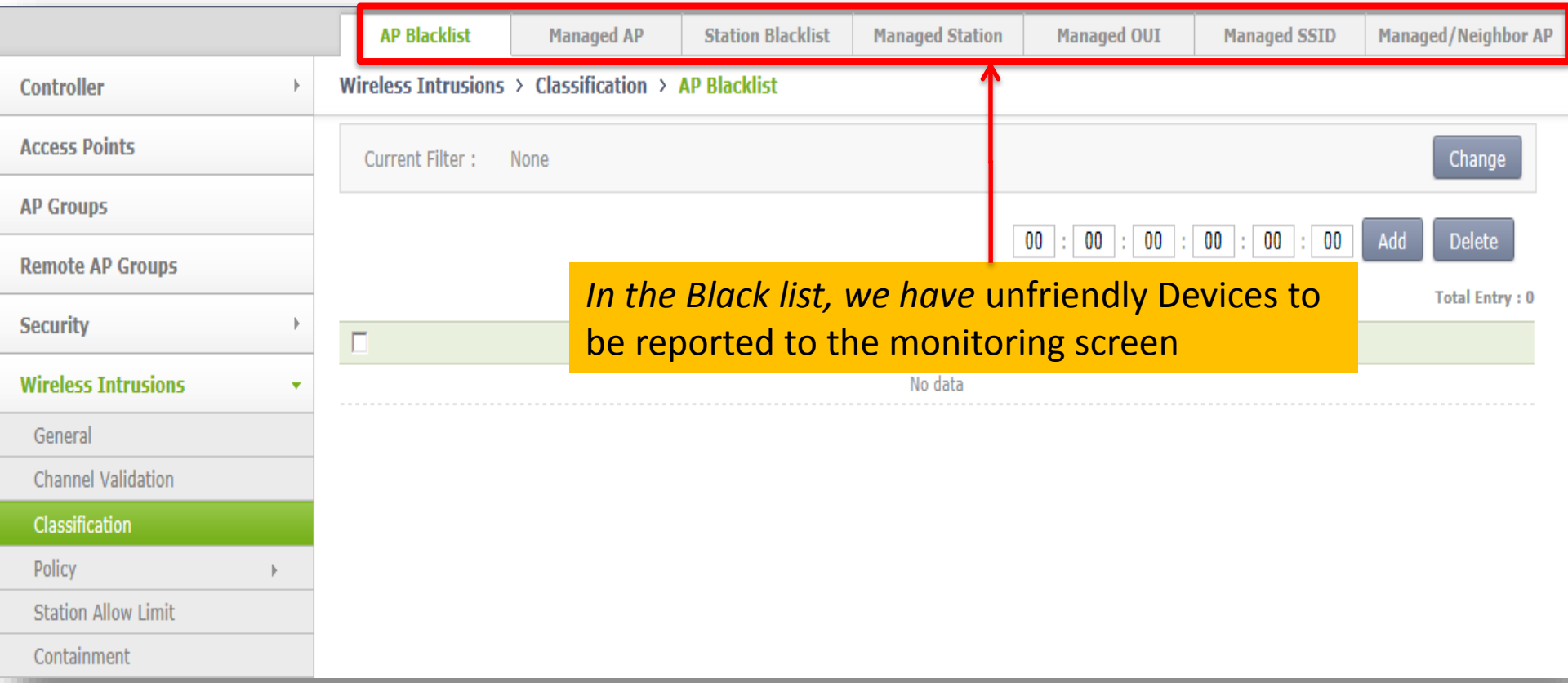


MAC ADDRESS	BSSID	SSID	CHANNEL NUMBER	STATUS	DETECTING AP
b4:b6:76:4b:64:05	00:00:00:00:00:00		0	Alert	f4:d9:fb:3d:e1:44
58:94:6b:63:f5:08	6c:f3:7f:95:e0:48	arrow-employee	48	Alert	f4:d9:fb:3d:e1:44
20:10:7a:03:70:0f	6c:f3:7f:95:e0:98	arrow-employee	149	Alert	f4:d9:fb:3d:e1:44
18:3d:a2:4a:6c:10	f4:d9:fb:3d:c0:e3	SamsungBCS	157	Alert	f4:d9:fb:3d:e1:44
20:10:7a:56:dd:13	f4:d9:fb:6a:01:20	SamsungNPI	161	Removed	f4:d9:fb:3d:e1:44
04:54:53:a8:44:1b	6c:f3:7f:95:e0:9b	STI-Mobile	149	Removed	f4:d9:fb:3d:e1:44
c8:d7:19:34:c7:1b	00:00:00:00:00:00		0	Alert	f4:d9:fb:3d:e1:44
88:53:2e:8f:a4:21	00:00:00:00:00:00		0	Alert	f4:d9:fb:3d:e1:44
c8:f7:33:d2:fa:23	00:00:00:00:00:00		0	Alert	f4:d9:fb:3d:e1:44
18:3d:a2:53:5f:30	f4:d9:fb:6a:01:20	SamsungNPI	161	Removed	f4:d9:fb:3d:e1:44
78:a3:e4:a6:c3:3f	6c:f3:7f:95:f2:33	STI-Mobile	11	Removed	f4:d9:fb:3d:e1:44
f4:b7:e2:3f:72:53	00:00:00:00:00:00		0	Alert	f4:d9:fb:3d:e1:44
08:3e:8e:87:fc:55	00:00:00:00:00:00		0	Alert	f4:d9:fb:3d:e1:44
64:a3:cb:43:1a:59	00:00:00:00:00:00		0	Alert	f4:d9:fb:3d:e1:44
40:0e:85:05:c3:5b	00:00:00:00:00:00		0	Removed	f4:d9:fb:3d:e1:44
d0:22:be:ba:b2:5d	f4:d9:fb:3d:c0:f0	SamsungBCS	11	Alert	f4:d9:fb:3d:e1:44
00:27:10:ce:1b:6c	f4:d9:fb:3d:c9:e2		161	Alert	f4:d9:fb:3d:e1:44
68:94:23:11:6f:6f	6c:f3:7f:95:e0:48	arrow-employee	48	Alert	f4:d9:fb:3d:e1:44
00:24:d2:14:16:82	f4:d9:fb:3d:c9:f1		1	Alert	f4:d9:fb:3d:e1:44
58:94:6b:f0:23:8c	6c:f3:7f:95:e0:98	arrow-employee	149	Removed	f4:d9:fb:3d:e1:44

2.6.2 Setup White/Black List



2.6.2 Setup Black List



Samsung Wireless Enterprise™

3. Advanced Deployment

- 3.1 Remote AP
- 3.2 Internal Radius Server
- 3.4 Quality of Service
- 3.5 VQM
- 3.6 Root and Repeater AP
- 3.7 SNMP

Samsung Wireless Enterprise™

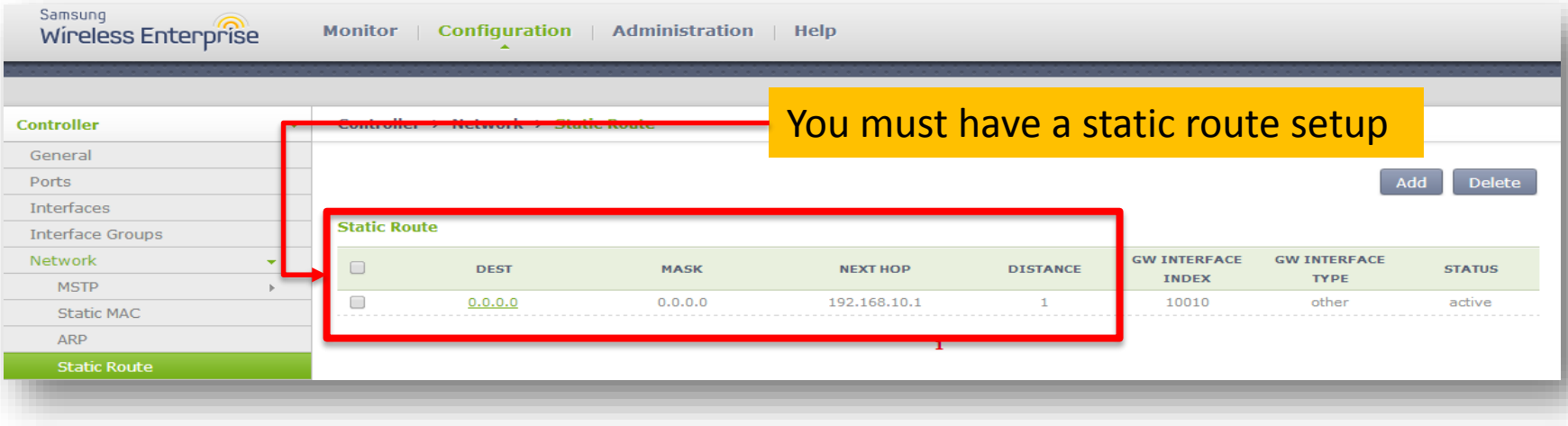
3.1 Remote AP

- 3.1.1 Firewall Ports
- 3.1.2 Public IP added
- 3.1.3 FTP Port
- 3.1.4 Remote AP Group
- 3.1.5 WLAN for Remote AP
- 3.1.6 CAPWAP Tunnel Mode
- 3.1.7 Remote AP “Scenario 1 and 2”

3.1.1 Firewall Ports

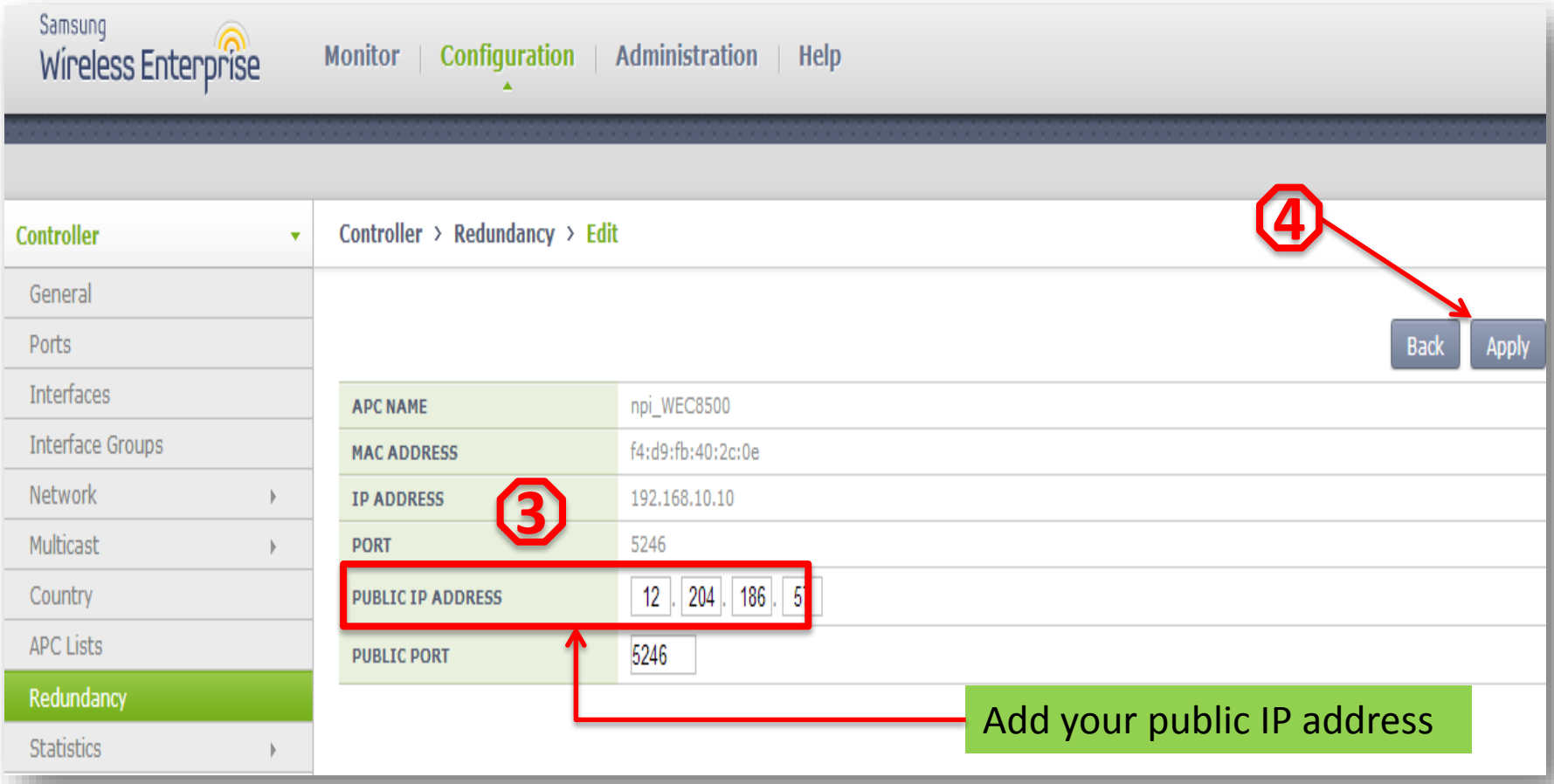
Please note the following must be configured on your firewall to allow the AP to connect to the CAPWAP IP address

- Port mapping must be setup on the following ports
  - 5246 udp
  - 5247 udp
- Example ***192.168.10.10 represents my CAPWAP IP***
  - policy 20 in address any any 12.13.14.15 32 protocol udp port any 5246 nat-ip 192.168.10.10
  - policy 21 in address any any 12.13.14.15 32 protocol udp port any 5247 nat-ip 192.168.10.10

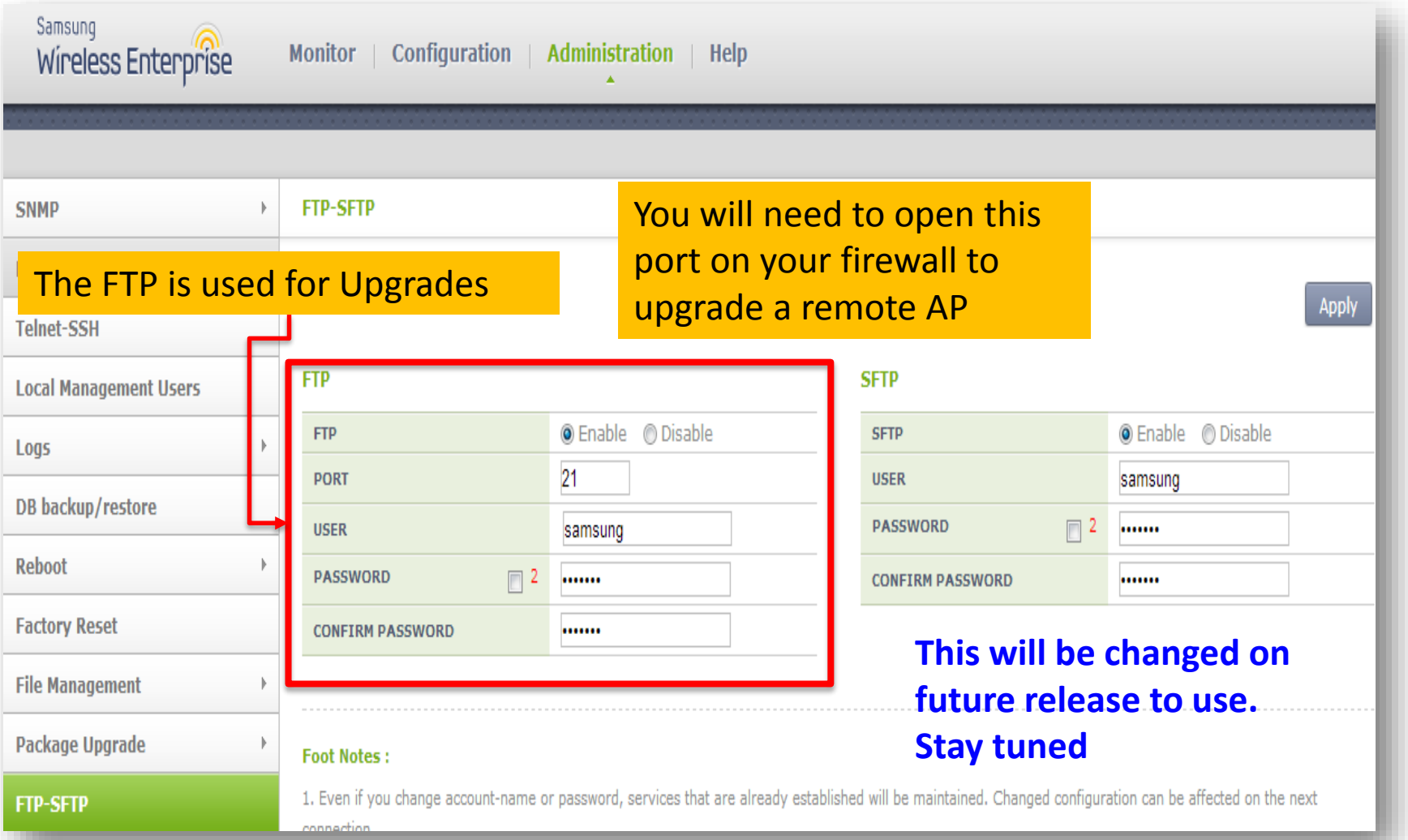


3.1.2 Public IP added

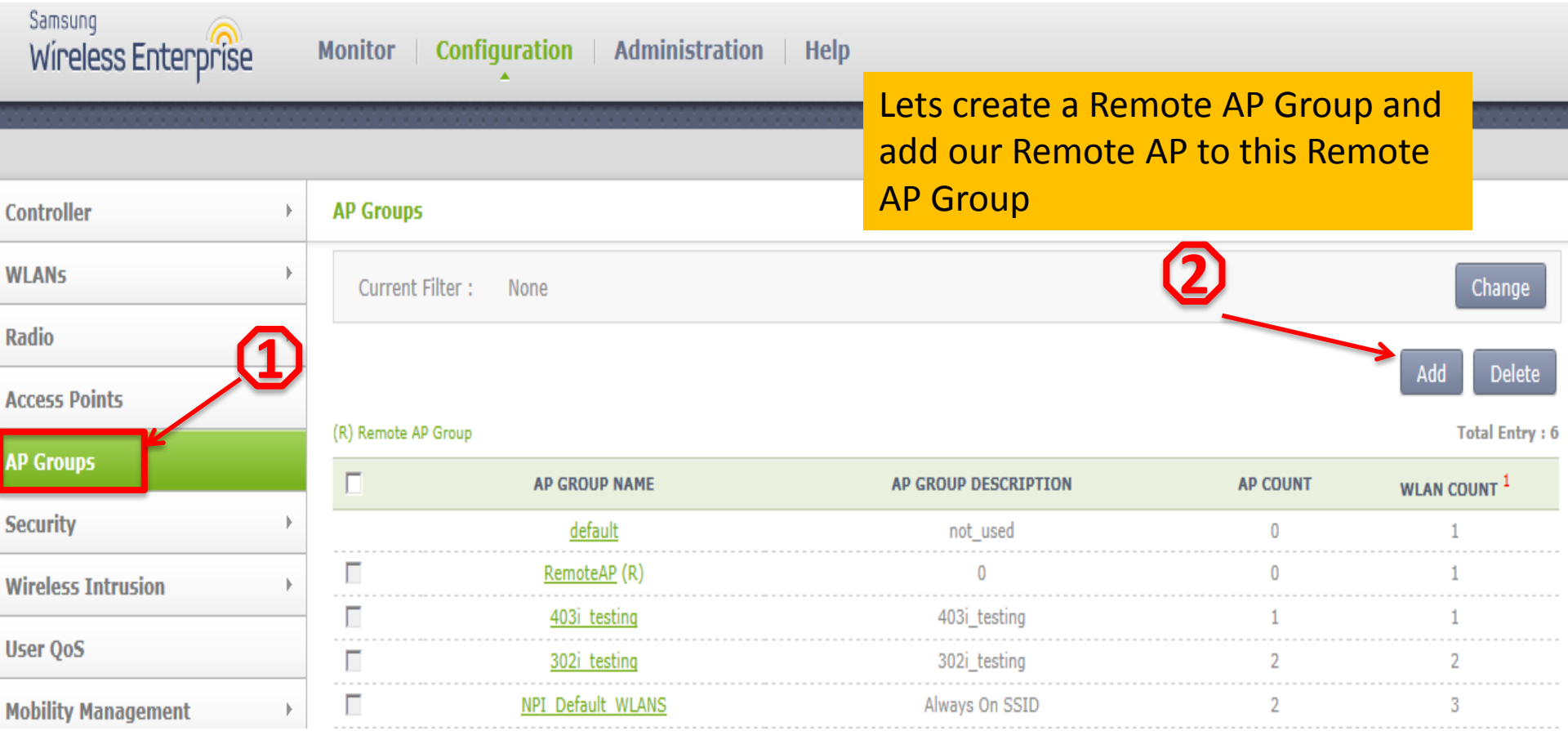
3.1.2 Public IP added



3.1.3 FTP Port

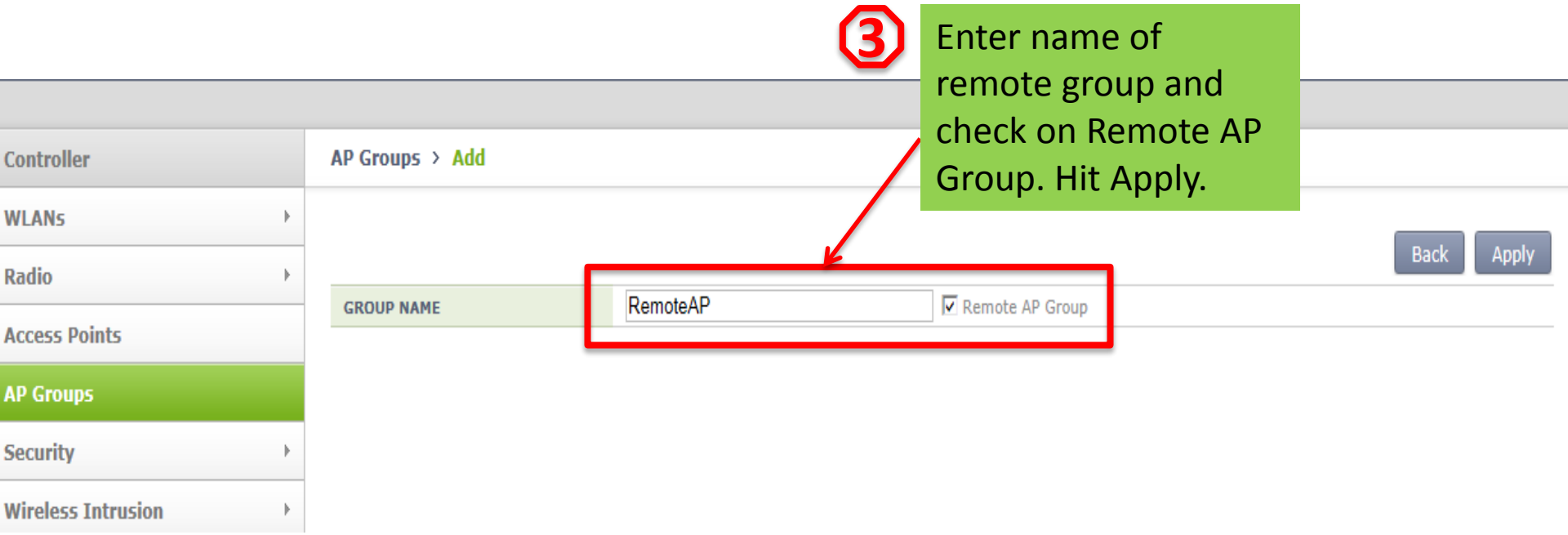

Samsung Wireless Enterprise
Monitor
Configuration
Administration
Help
SNMP
Telnet-SSH
Local Management Users
Logs
DB backup/restore
Reboot
Factory Reset
File Management
Package Upgrade
FTP-SFTP
FTP-SFTP
The FTP is used for Upgrades
You will need to open this port on your firewall to upgrade a remote AP
Apply
FTP
FTP
Enable
Disable
PORT
21
USER
samsung
PASSWORD
2
CONFIRM PASSWORD
SFTP
SFTP
Enable
Disable
USER
samsung
PASSWORD
2
CONFIRM PASSWORD
This will be changed on future release to use. Stay tuned
Foot Notes :
1. Even if you change account-name or password, services that are already established will be maintained. Changed configuration can be affected on the next connection

3.1.4 Remote AP Group



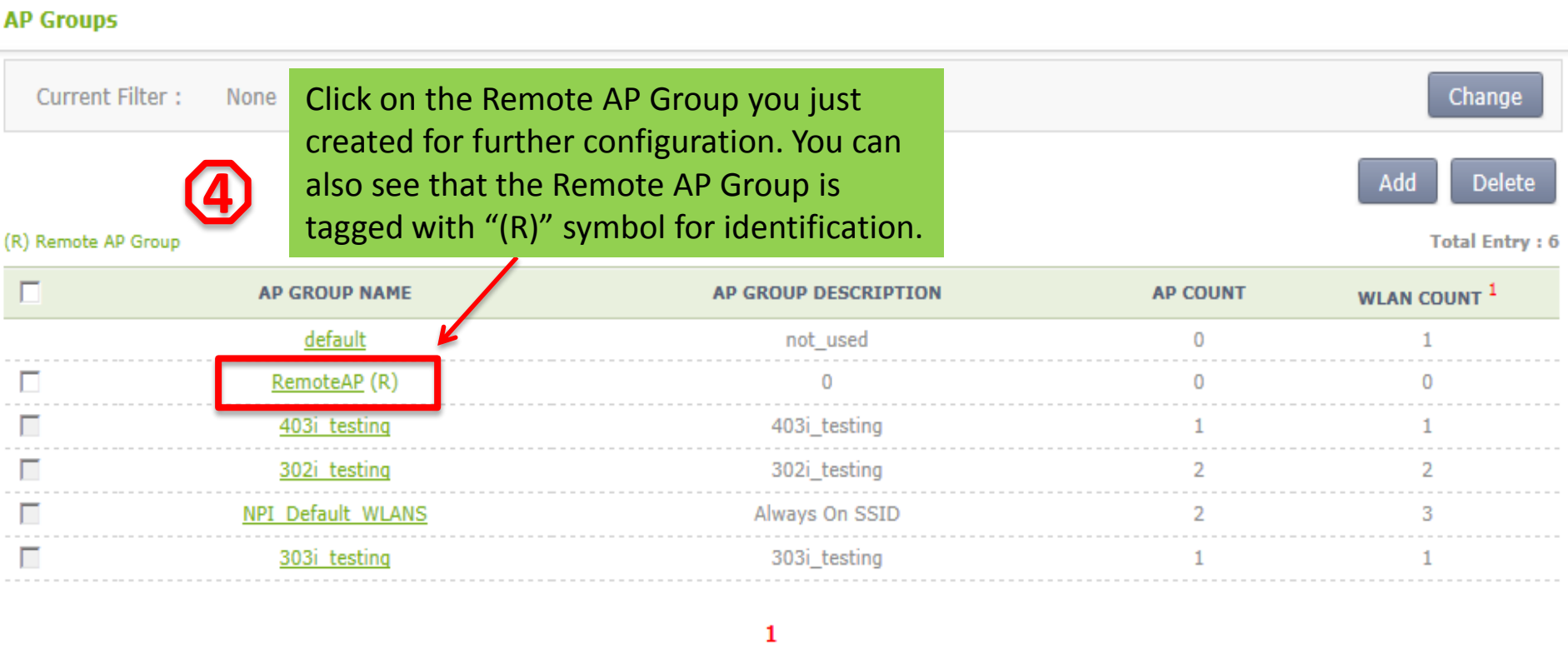
3.1.4 Remote AP Group

Samsung Wireless Enterprise™



3.1.4 Remote AP Group

Samsung Wireless Enterprise™



3.1.4 Remote AP Group

Samsung Wireless Enterprise™

General | APs | WLANs | 802.11a/n | 802.11b/g/n | Remote AP Group | Advanced

AP Groups > APs

Back

AP GROUP NAME	RemoteAP

Current Filter : None

4

Change

Selected APs

Total Entry : 0

AP PROFILE NAME	AP NAME	MAC ADDRESS	IP ADDRESS	LOCAL AUTH. LIST STATUS
No data				

Here you can select which AP will be in this Remote AP Group and then hit the Up Arrow button.

▽ △

Change

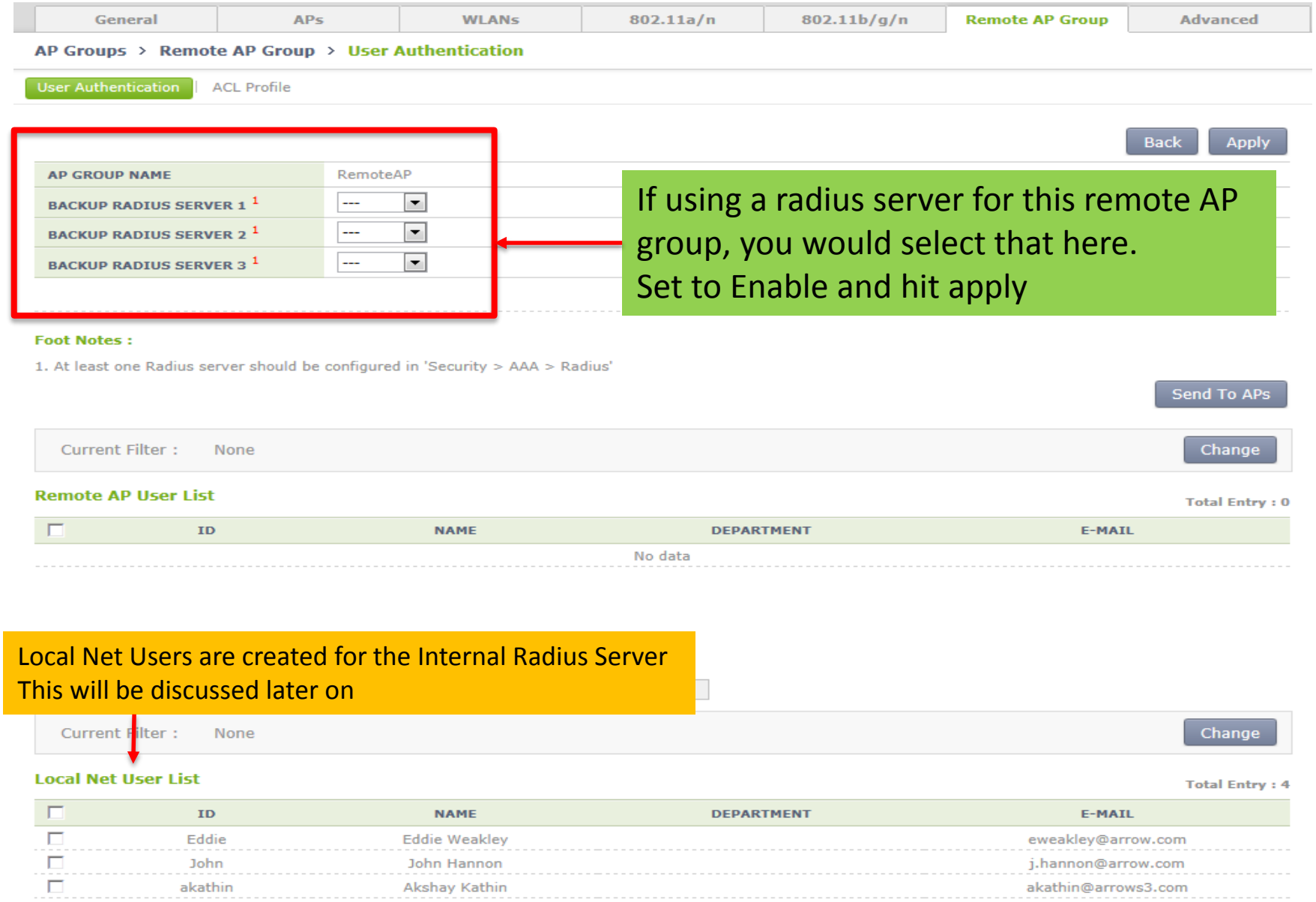
All APs

Total Entry : 6

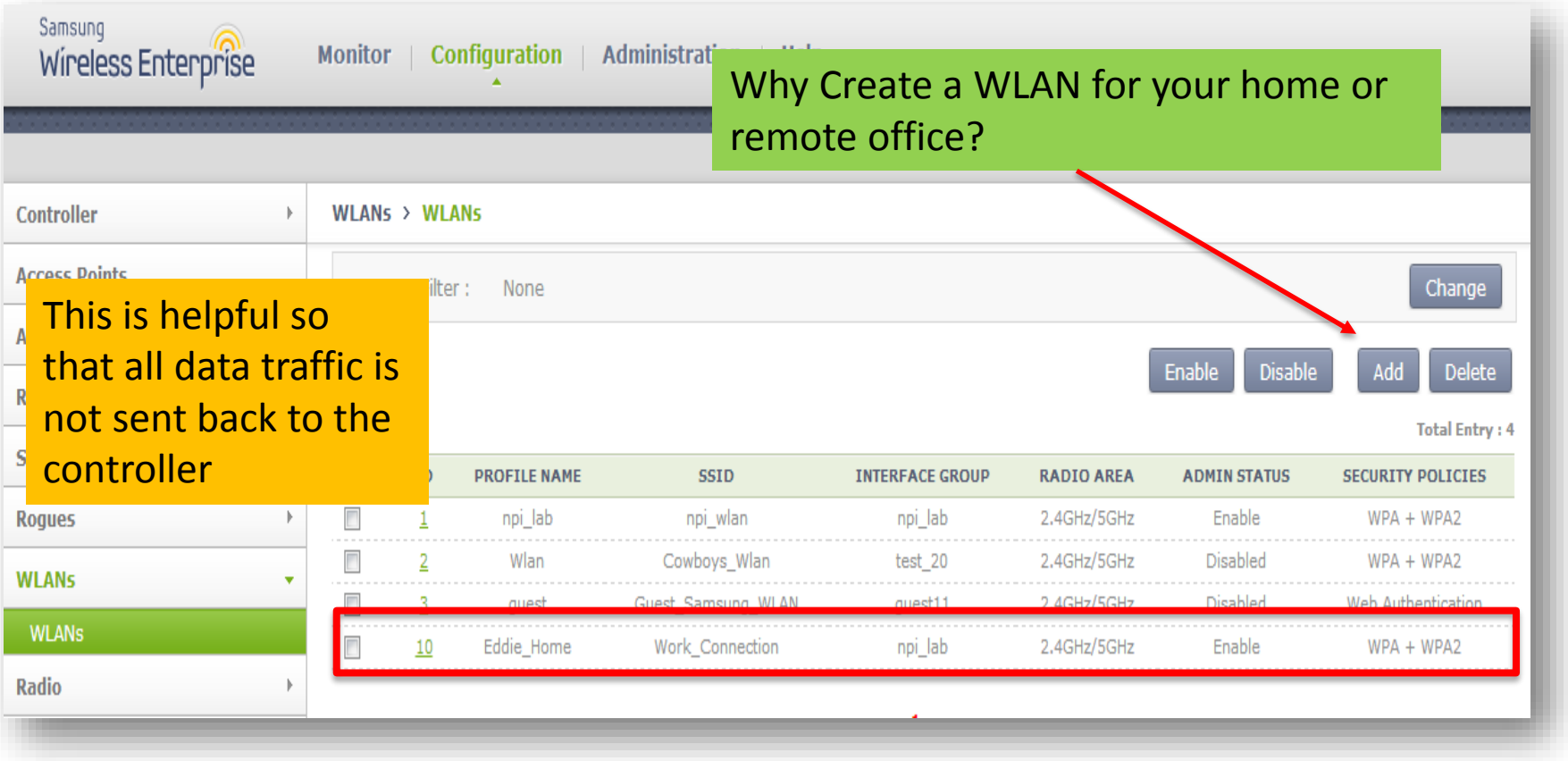
AP PROFILE NAME	AP NAME	MAC ADDRESS	IP ADDRESS	AP GROUP NAME
ap_1	npi_Lab_AP	f4:d9:fb:3d:c4:84	0.0.0.0	302i_testing
ap_2	npi_302i_AP2	f4:d9:fb:3d:e1:44	0.0.0.0	302i_testing
ap_3	npi_403i_AP	f4:d9:fb:6a:01:03	0.0.0.0	403i_testing
ap_4	npi_303i_AP	f4:d9:fb:69:d5:61	192.168.10.117	303i_testing
ap_7	npi_412i_AP	f4:d9:fb:69:eb:c3	0.0.0.0	NPI_Default_WLANS

3.1.4 Remote AP Group

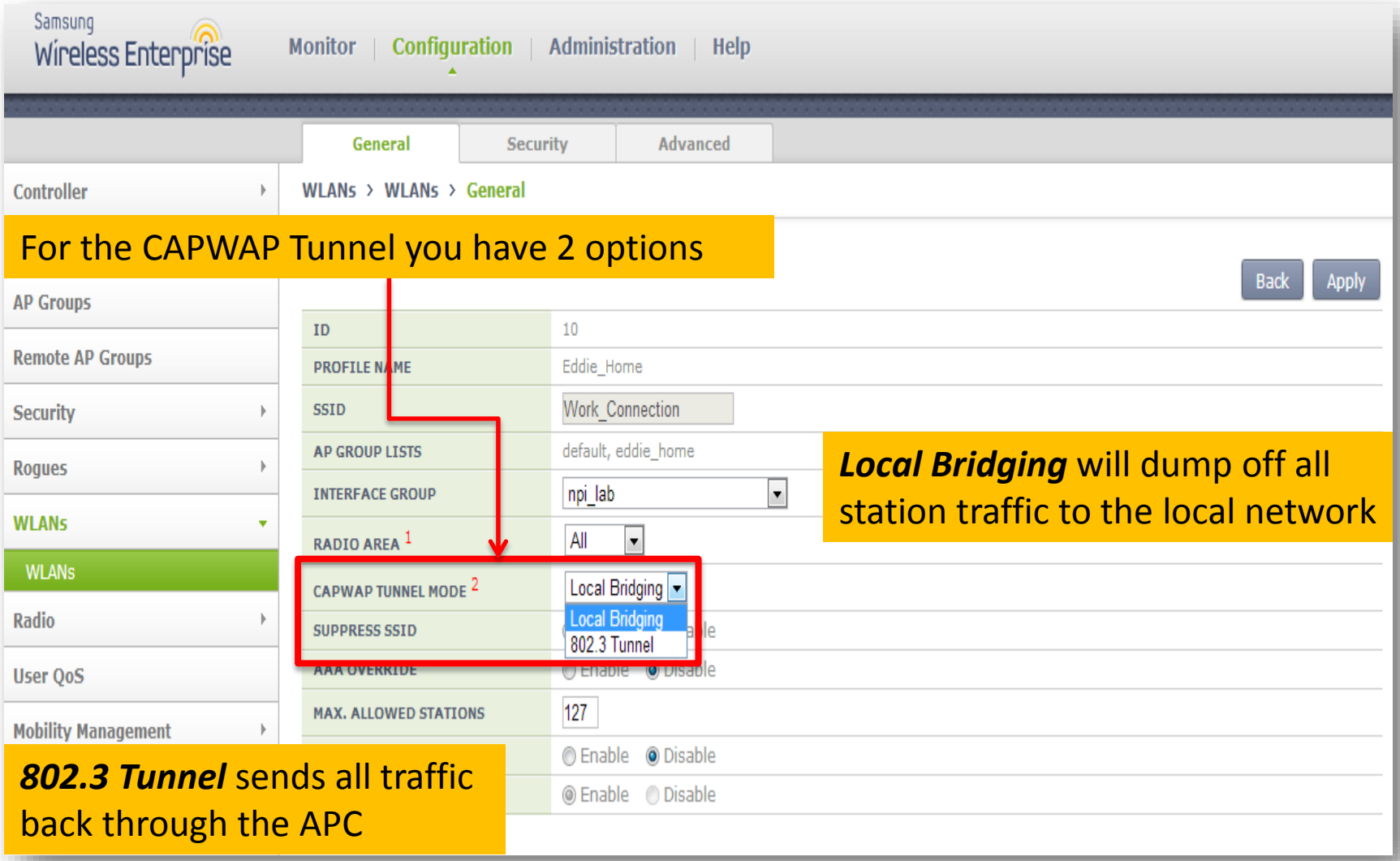
Samsung Wireless Enterprise™



3.1.5 WLAN for Remote AP

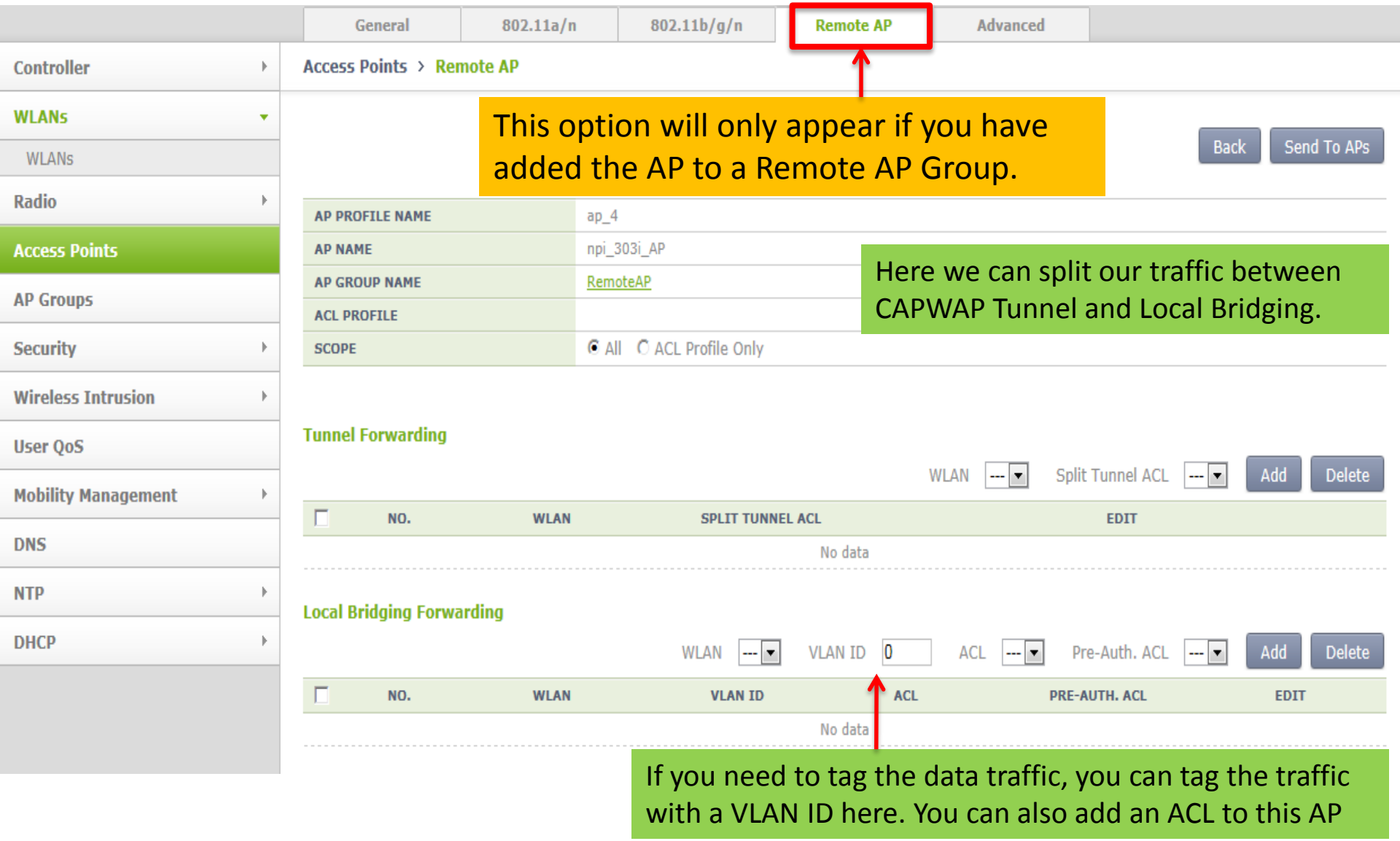


3.1.6 CAPWAP Tunnel Mode



3.1.6 CAPWAP Tunnel Mode

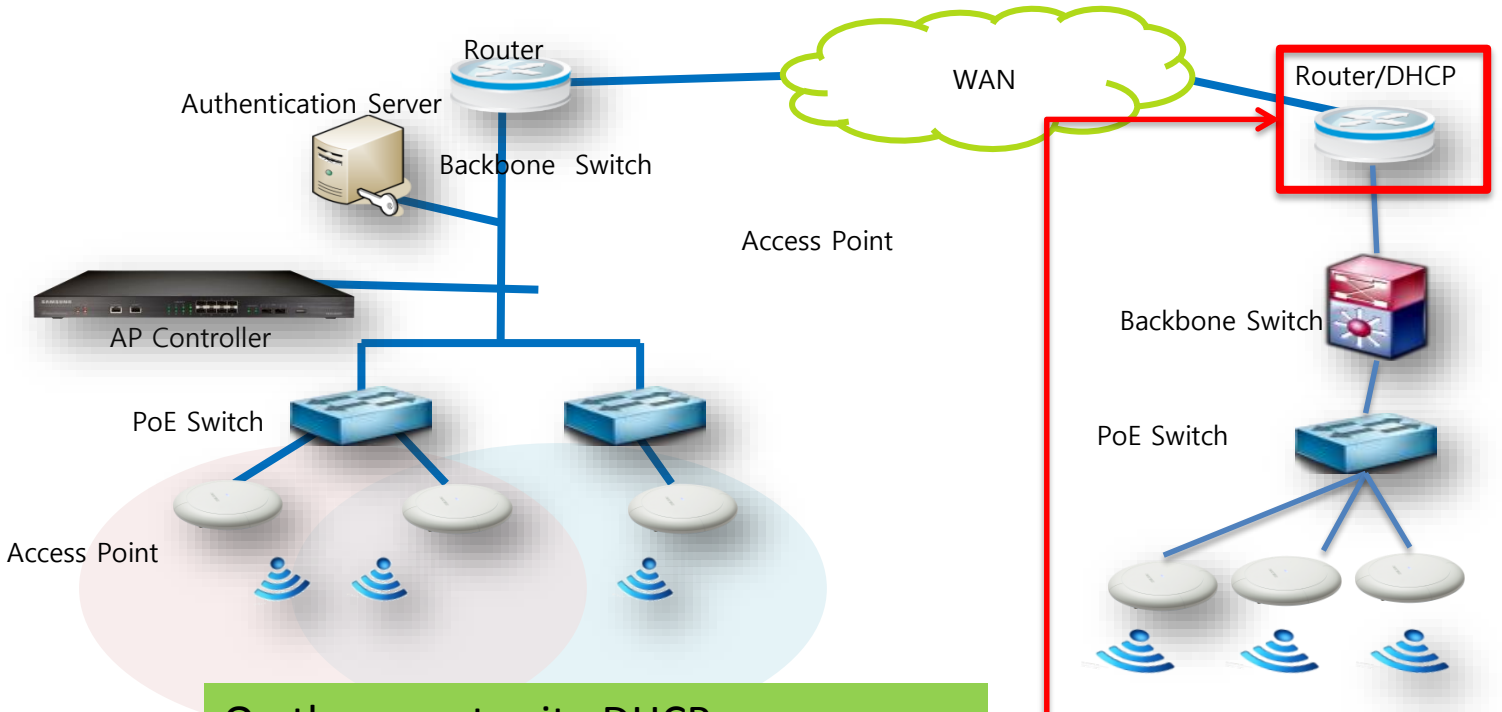
Samsung Wireless Enterprise™



3.1.7 Remote AP “Scenario 1”

Samsung Wireless Enterprise™

You have a remote office with multiple AP’s at the remote office



On the remote site DHCP server we need to add the user_option 138 into the DHCP server

3.1.7 Remote AP “Scenario 1”

Samsung Wireless Enterprise™

Example -

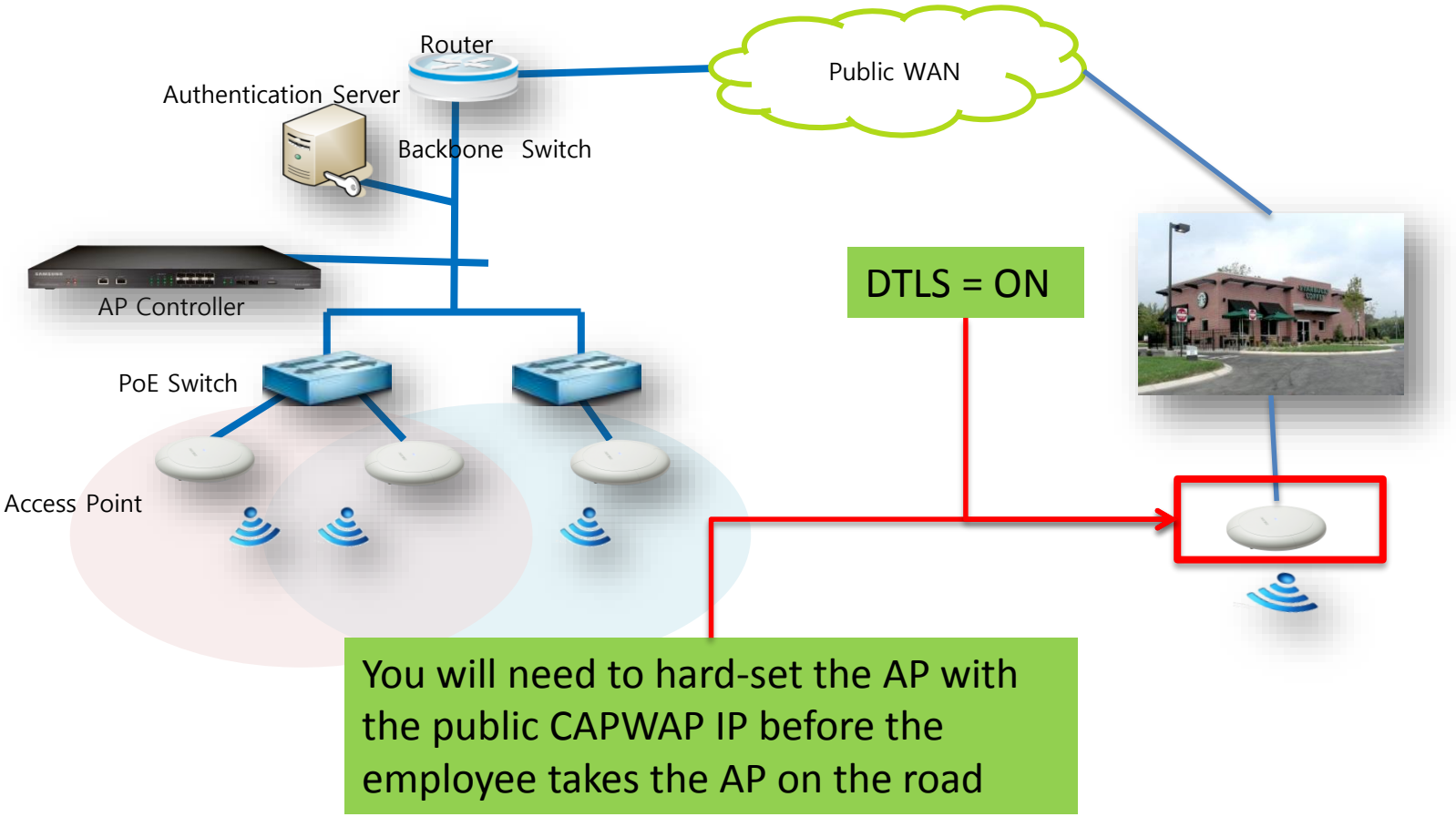
```
pool remoteoffices
    domain abc.com
    dnsserver 8.8.8.8
    network 192.168.111.0 255.255.255.0
    default_router 192.168.111.1
    exclude-range 192.168.111.1 192.168.111.20
    user_option 138 ipaddress 12.13.14.15 active
    commit
    exit pool
```

This IP address should be the CAPWAP IP address, here we are using the public IP
If you have a MPLS between sites, then you would use the local CAPWAP IP address instead

3.1.7 Remote AP “Scenario 2”

Samsung Wireless Enterprise™

You have a remote employee that uses an AP while out of office from many different location



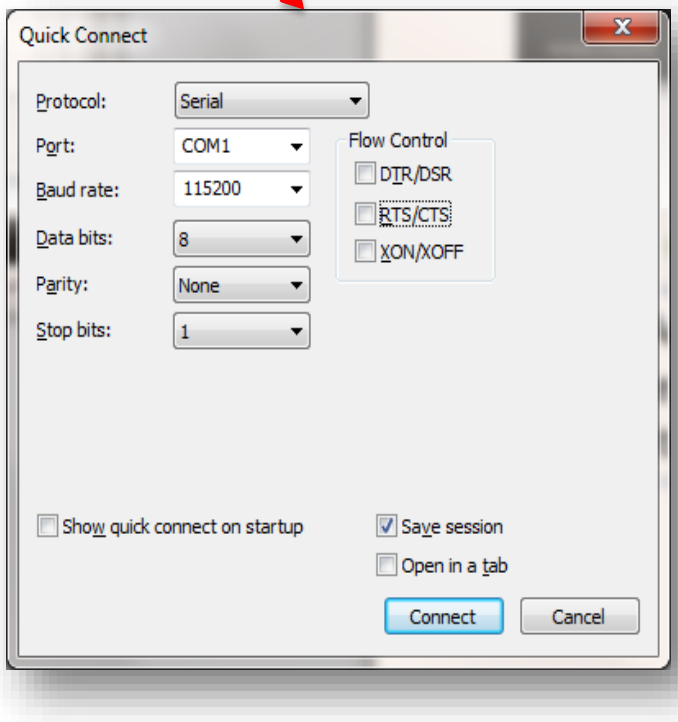
Samsung Wireless Enterprise™

Hard Setting the CAPWAP IP Address -

Statically assign the CAPWAP IP to an AP

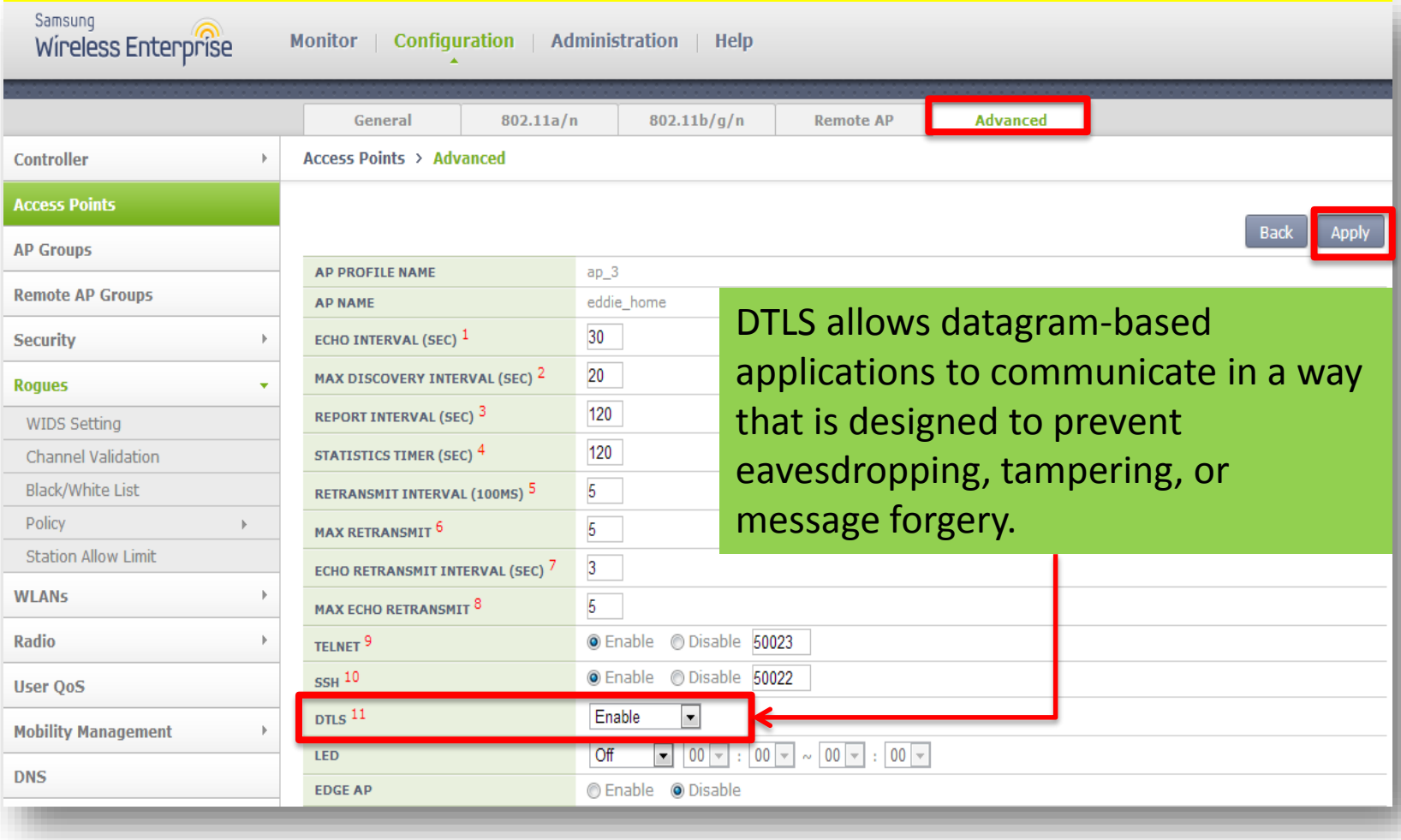
1. Connect the Samsung Rollover cable to the console port of the AP
2. Login Name = root
3. Password = samsung
4. Warehouse_Root# config capwap apcIP 12.204.186.56
5. Warehouse_Root # config save

You must perform a save command after making this change



3.1.7 Remote AP “Scenario 2”

Samsung recommends that you turn this on for Security in the event that the AP is not behind a corporate firewall



Lab 19 – (1/3)

Setup an Remote AP

1. Go to Configuration → Controller → Redundancy
   - Click on the name of your APC
   - Update the public IP address = 12.204.186.56 → Hit Apply
2. Go to Configuration → Controller → Network → Static Route
   - Verify that a Static route has been added
3. Go to Configuration → AP Groups
   - Create a Remote Group called “home_group”
   - Click on name of Group
   - Add one of your AP’s to this group → Hit Apply
4. Go to Configuration → Access Points → Click on the AP you placed in the Remote Group
   - Click on the Advanced Tab → Set Telnet to Enable and hit Apply

Lab 19 – (2/3)

Setup an Remote AP

1. Next, Telnet to the Access Point you wish to make a Remote AP
   - Telnet to the APC First 192.168.xx.10
   - Enter login and password
   - WEC8500#show ap summary

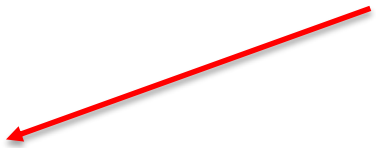
```
WEC8500# show ap summary

 AP Mgmt interface IP : 192.168.10.10 (vlan1.10)

 AP_ID   Profile        AP_NAME          MAC_Address        IPv4Addr       State Speed Duplex   Location   Country(Model Type)
====== ========== ================== ================= =============== ===== ===== ====== ========== ==================
     1       ap_1      npi_Lab_AP f4:d9:fb:3d:c4:84   192.168.10.100 1/1/5   100   Full      npi_lab  US (Unknown)
     2       ap_2      Eddie_Home f4:d9:fb:3d:e1:44    192.168.0.114 1/1/5   100   Full   Carrollton  US (Unknown)
     3       ap_3         AP_303i f4:d9:fb:36:ca:af   192.168.10.102 1/1/5   100   Full EddieDeskTop  US (Unknown)
     4       ap_4     Student4_AP1 f4:d9:fb:3d:a5:96   192.168.10.105 1/1/5   100   Full     Anywhere  US (Unknown)
     5       ap_5     Student4_AP2 f4:d9:fb:3d:94:96   192.168.10.104 1/1/5   100   Full         Root  US (Unknown)
WEC8500#
```

2. Telnet to the AP you added to the remote AP Group
   - Example = WEC8500#telnet 192.168.10.100 50023
   - Login = root
   - Password = samsung

Lab 19 – (3/3)

Setup an Remote AP

Statically set your CAPWAP IP



1. Configure a static capwap IP
   - Student4_AP5# config capwap apcIP 192.168.xx.10
   - Student4_AP5# config Connection closed by foreign host.
2. Next, unplug the AP and plug in the remote Network
   - In classroom, plug your AP into neighbors port 1-16
3. Go to Configuration → Access Points → See that your AP has registered.

4. Lastly, default the AP and set back to normal
   - First, unplug from the AP from the remote network and plug back into your local network. (port 17-24)
   - You must connect via console to Default an AP
   - Go to Configuration → Access Points → Click on the AP you placed in the Remote Group
   - Click on the Advanced Tab → Set Console to Enable and hit Apply
5. Connect to the AP via Console Cable
   - Login = root
   - Password = samsung
   - Student4_AP1# system factory reset ip aft
   - Factory Set ..
   - System was reset without network informations
6. After the AP comes back to the login screen,

3.2 Internal Radius Server

Samsung Wireless Enterprise™

3.2 Internal Radius Server

- 3.2.1 Local Net Users
- 3.2.2 Creating a LN Users
- 3.2.3 Assigning to a WLAN
- 3.2.4 Windows Settings

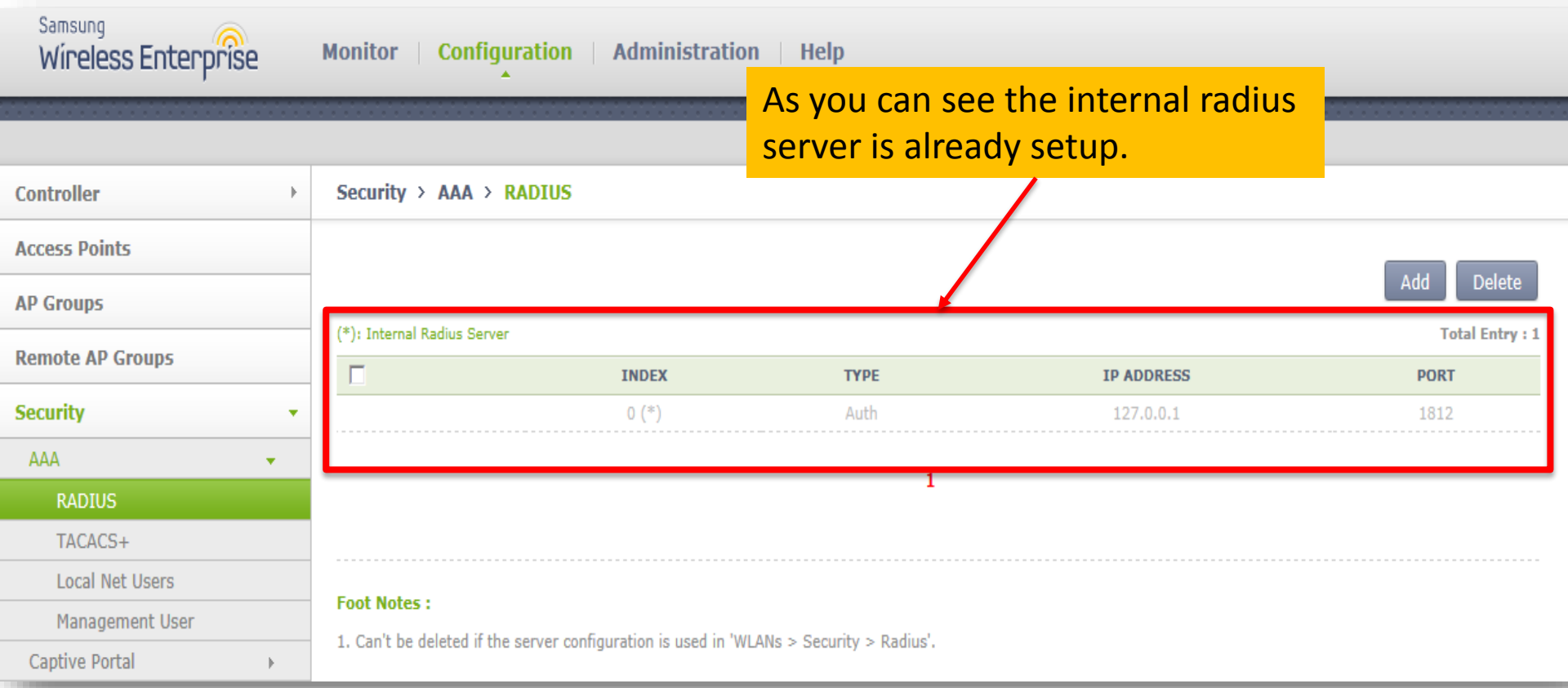
Internal RADIUS Server

The Samsung wireless LAN system provides the security and authentication function by interoperating with an internal RADIUS server.

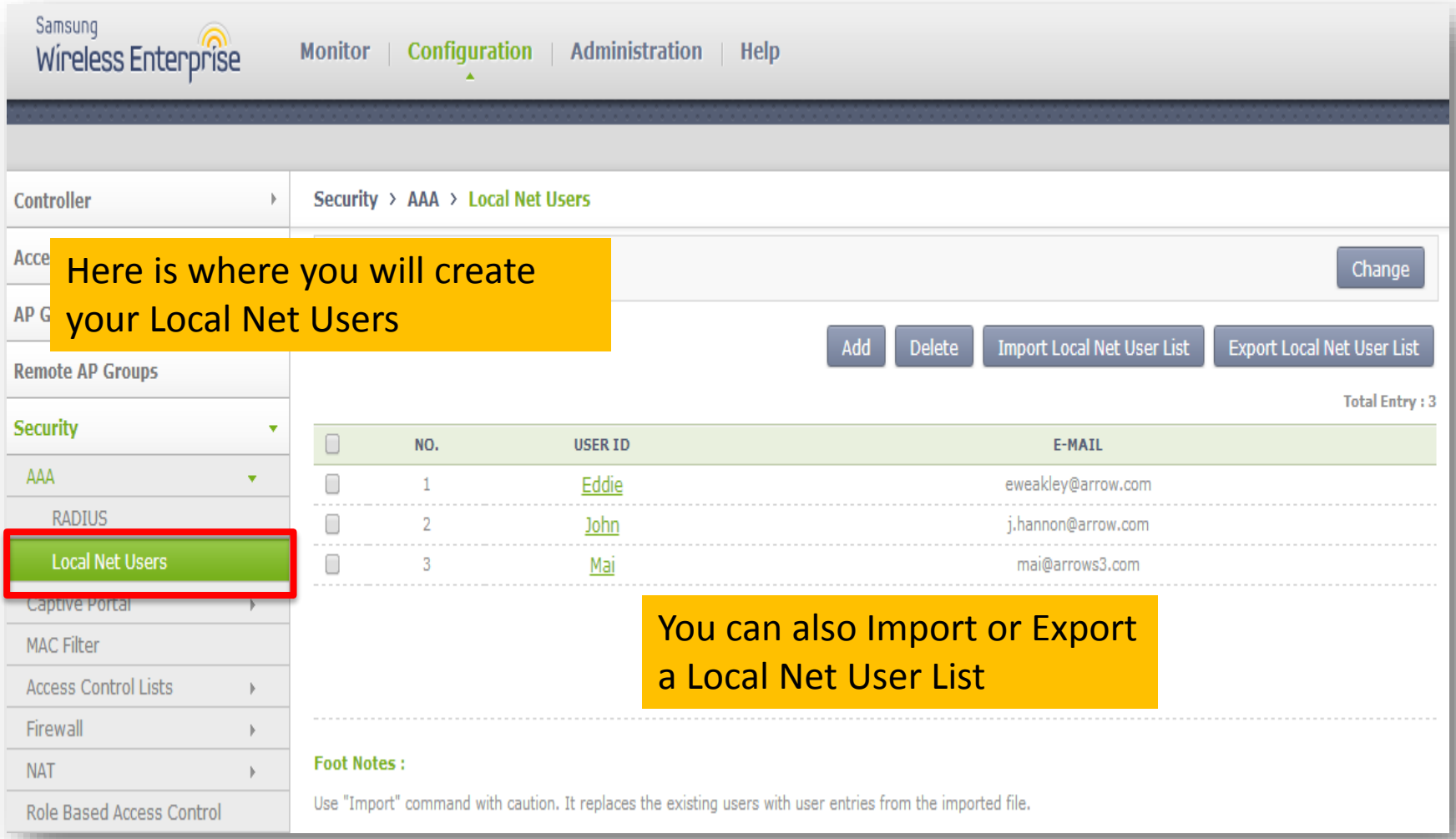
The internal RADIUS server is supported on the WEC8050 and the WEC8500.

To use the internal RADIUS server, operator can add, delete, or edit a user (maximum 512 users).

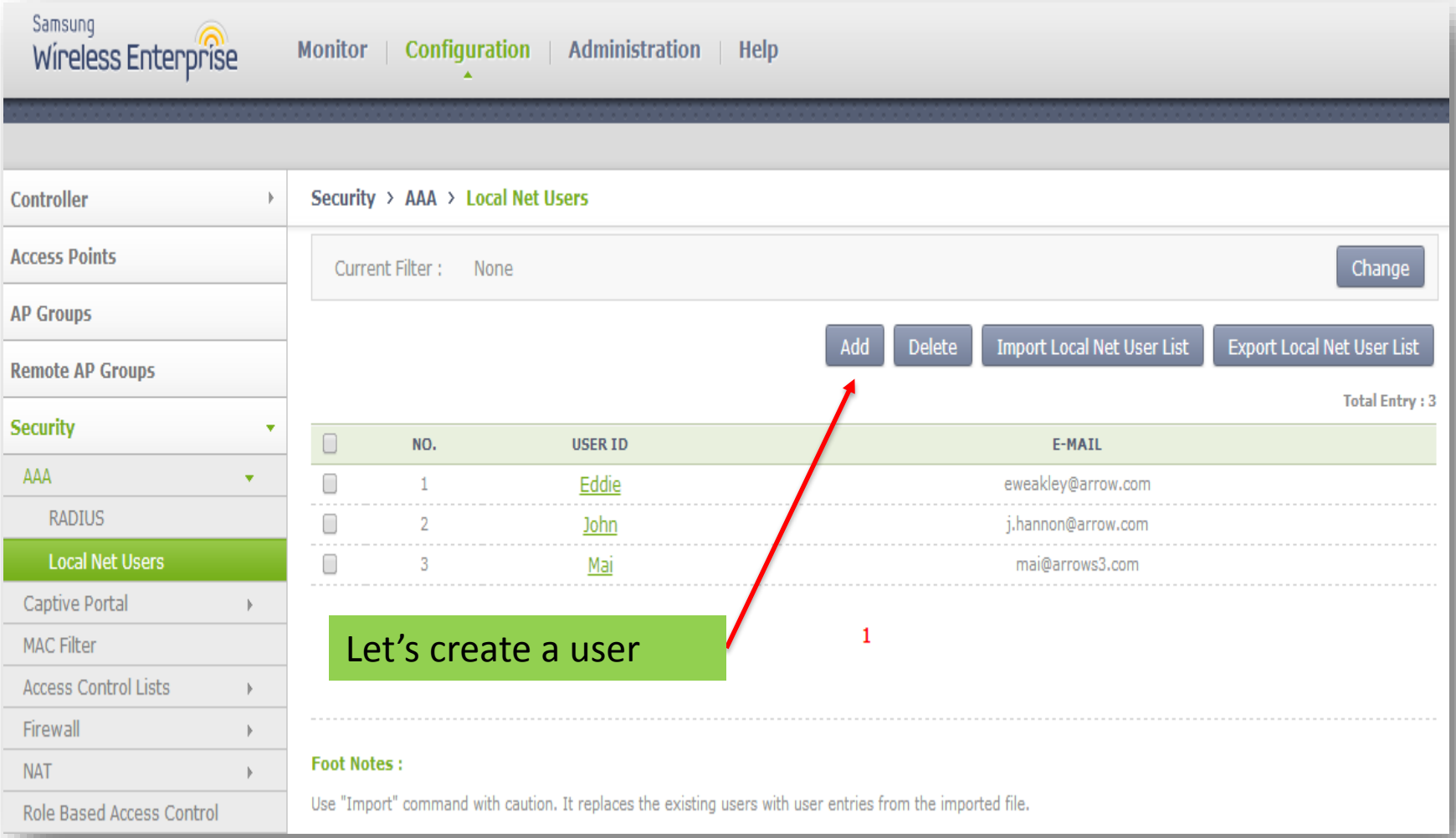
3.2 Internal Radius Server



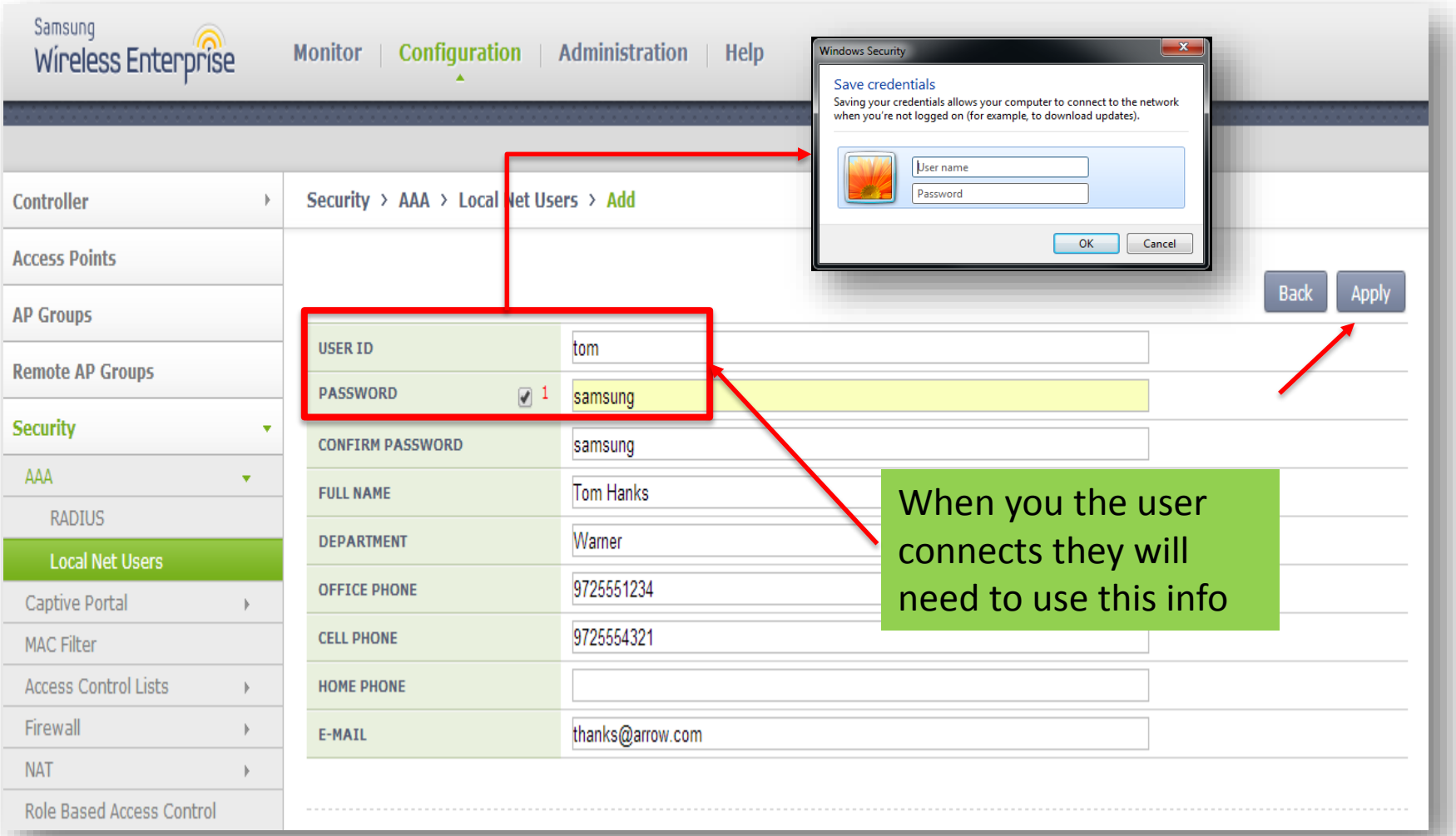
3.2.1 Local Net Users



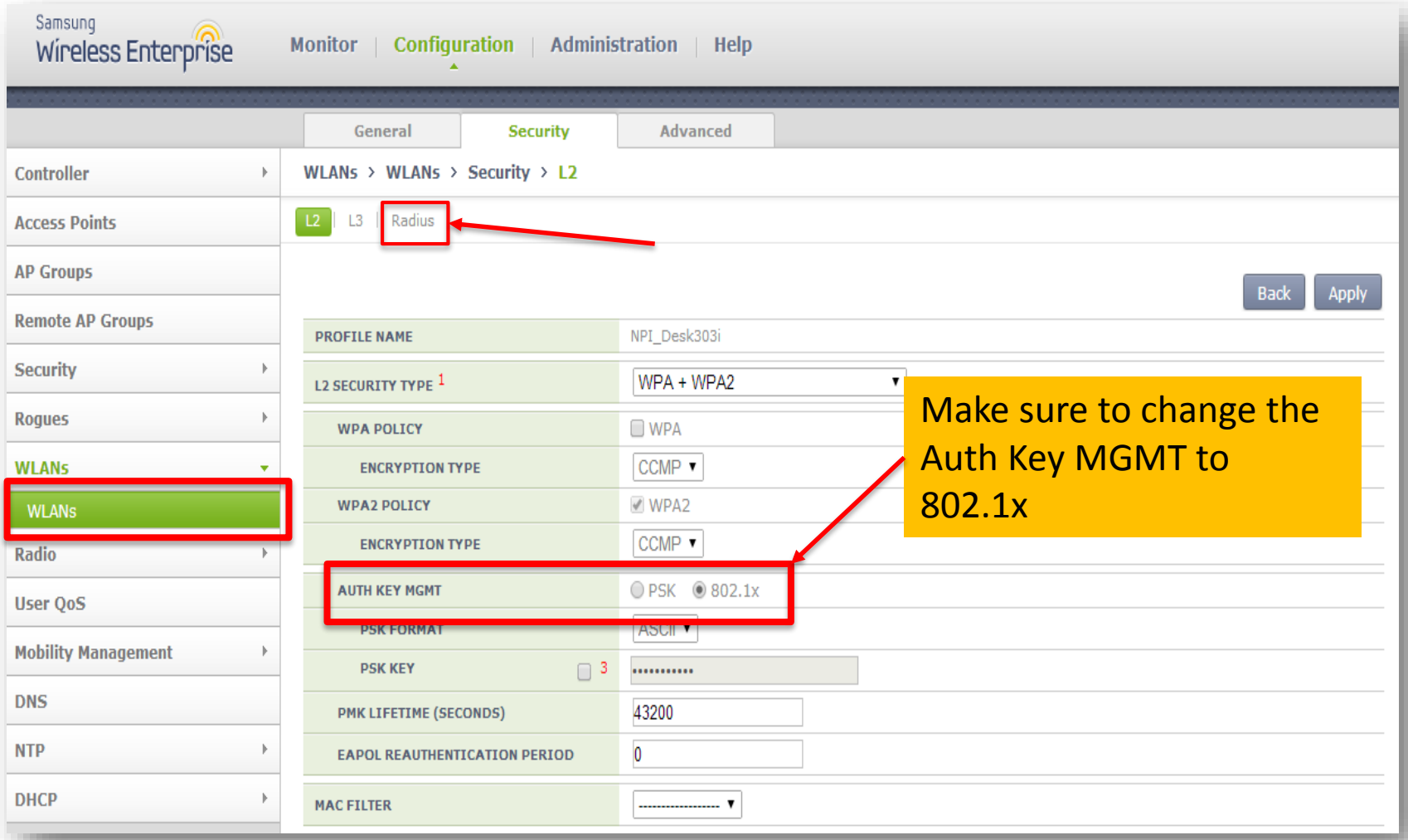
3.2.2 Creating a LN Users



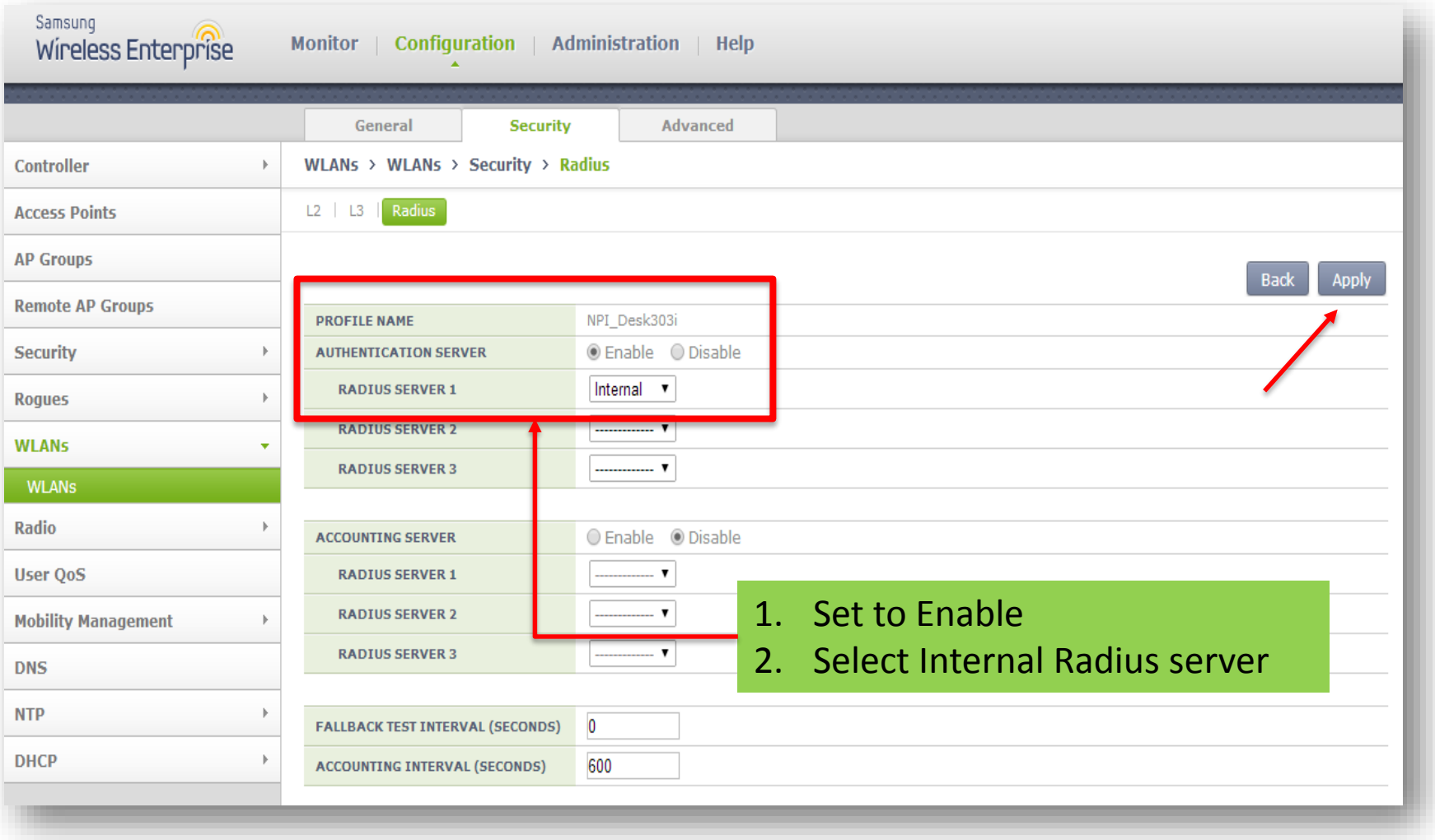
3.2.2 Creating a LN Users



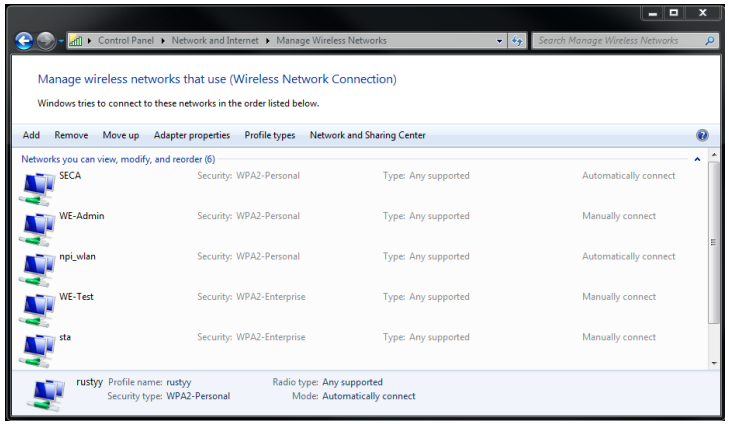
3.2.3 Assigning to a WLAN



3.2.3 Assigning to a WLAN

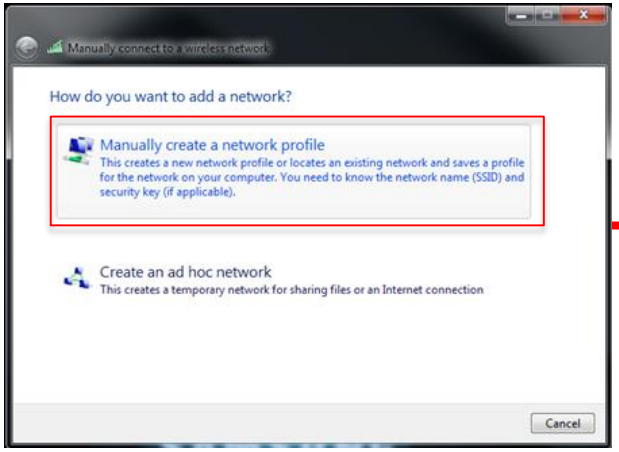


3.2.4 Windows Settings

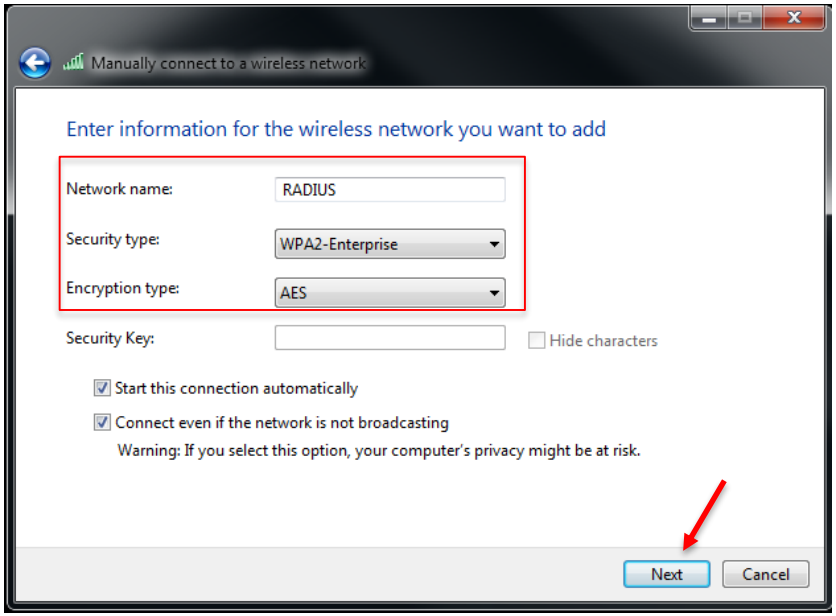


Open “Manage Wireless Networks” Control Panel

Click Add a wireless network

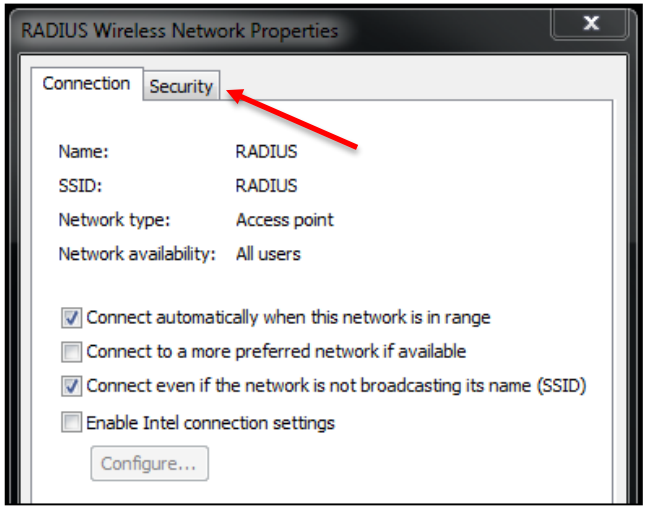


Select “Manually create a network profile”

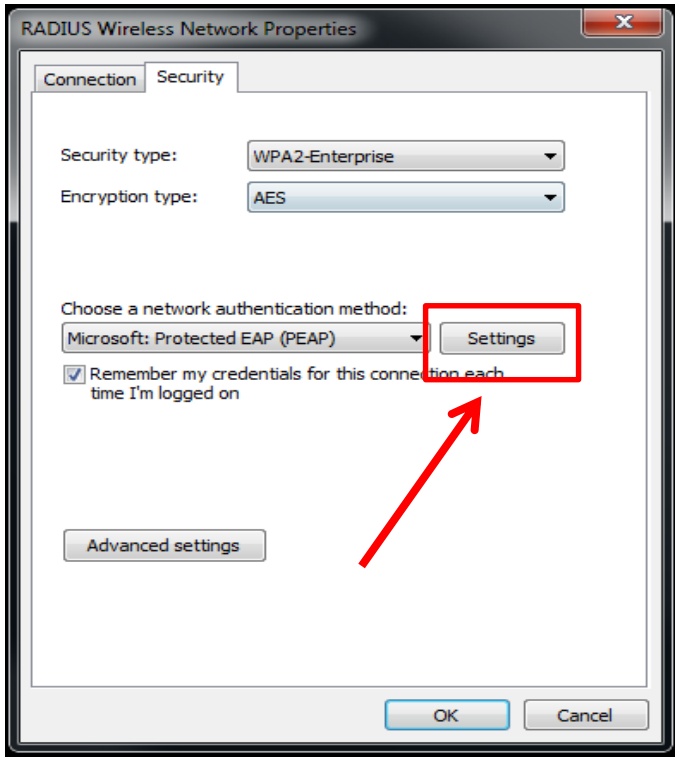


Enter SSID and select WPA-2 Enterprise/AES
Optional: Connect even if the network is not broadcasting

3.2.4 Windows Settings

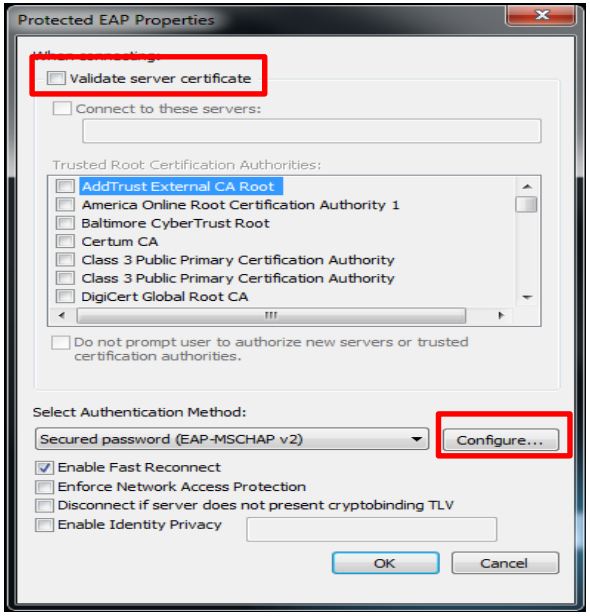


Edit connection settings

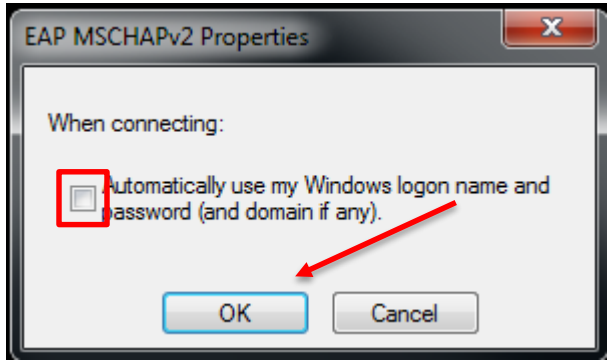


Select Security Settings

3.2.4 Windows Settings

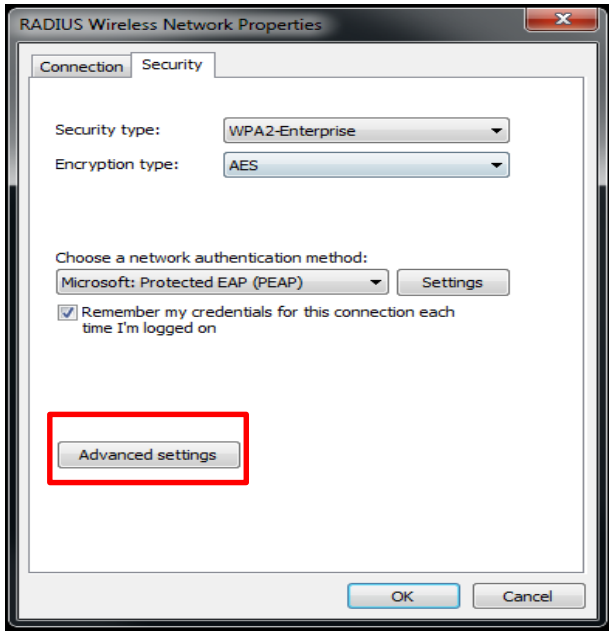


Uncheck Validate server Certificate
Select Configure Authentication Method

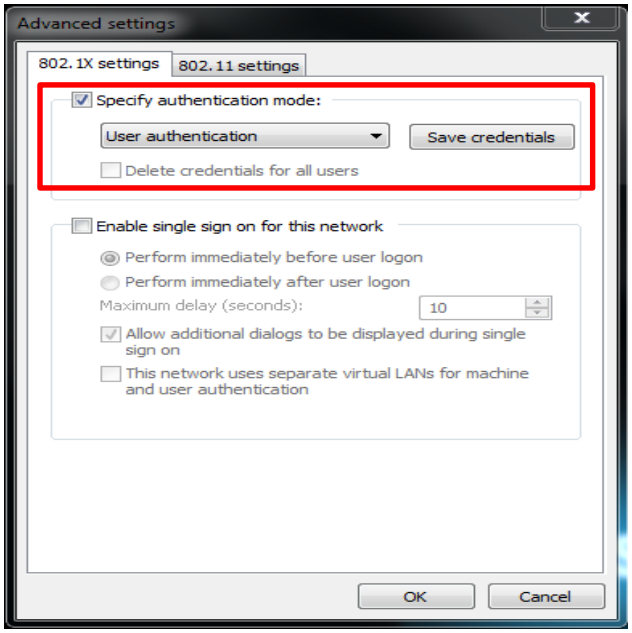


Uncheck windows logon credentials

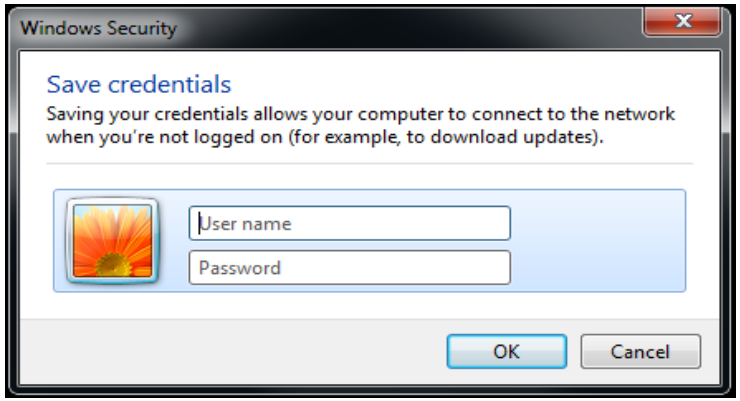
3.2.4 Windows Settings



Select Security Advanced Settings



Select "Specify Auth Mode"
Select User Auth
Select Save Credentials



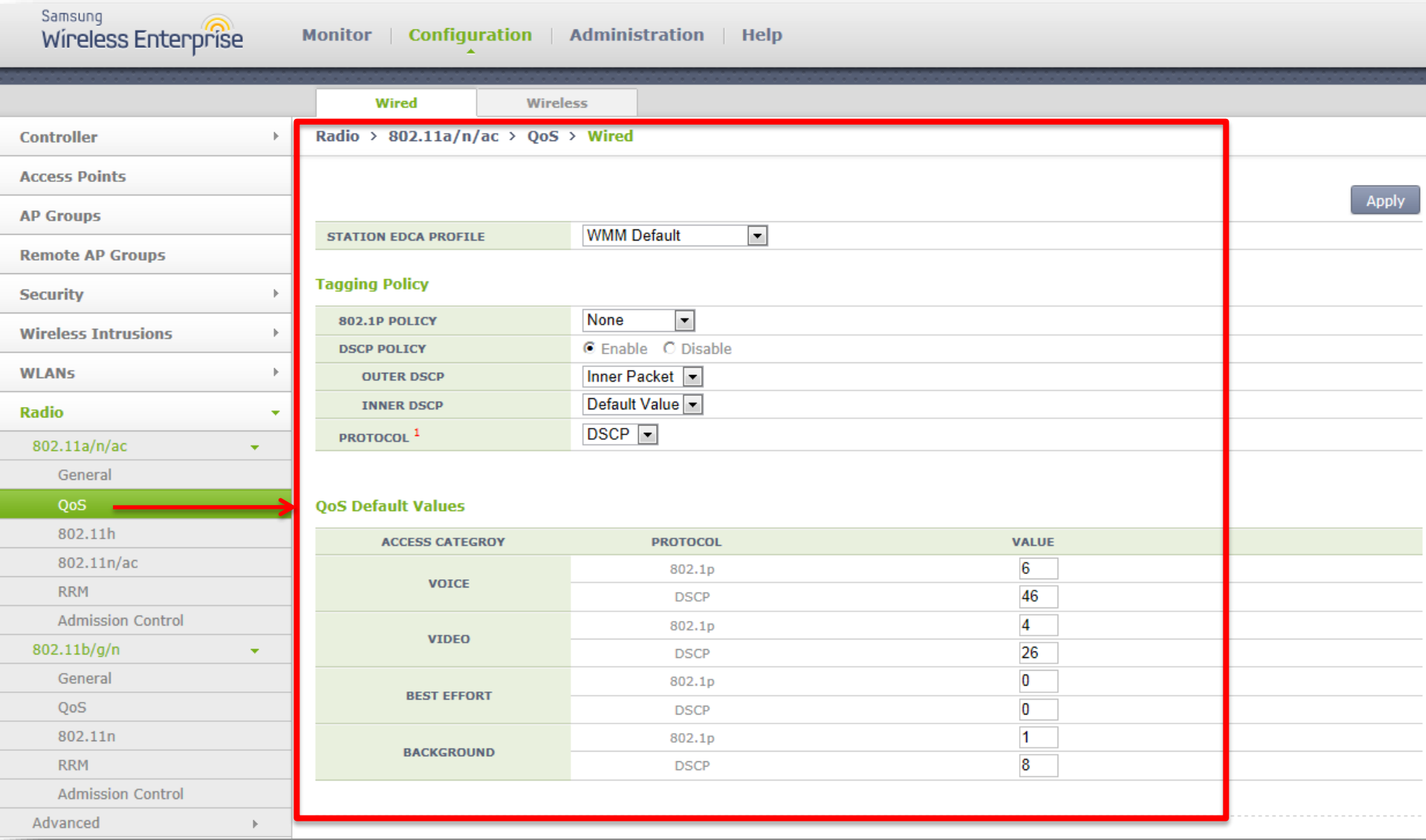
Enter your Internal RADIUS credentials

Connect to Network

Quality of Service (DSCP)

3.4 Quality of Service

Samsung Wireless Enterprise™



Samsung Wireless Enterprise™

3.5 VQM

- 3.5.1 Voice Quality Monitoring
- 3.5.2 Features of VQM
- 3.5.3 Configuration for VQM
- 3.5.4 Monitoring Voice Traffic

3.5.1 Voice Quality Monitoring

Samsung Wireless Enterprise™

The WEC8500 provides the Voice Quality Monitoring (VQM) function as an additional service.

As a function that monitors a voice packet in real-time, the VQM checks and manages the voice quality of a voice call being service by using the current wireless LAN section and also provides the status information by monitoring the quality of a voice traffic.

3.5.2 Features

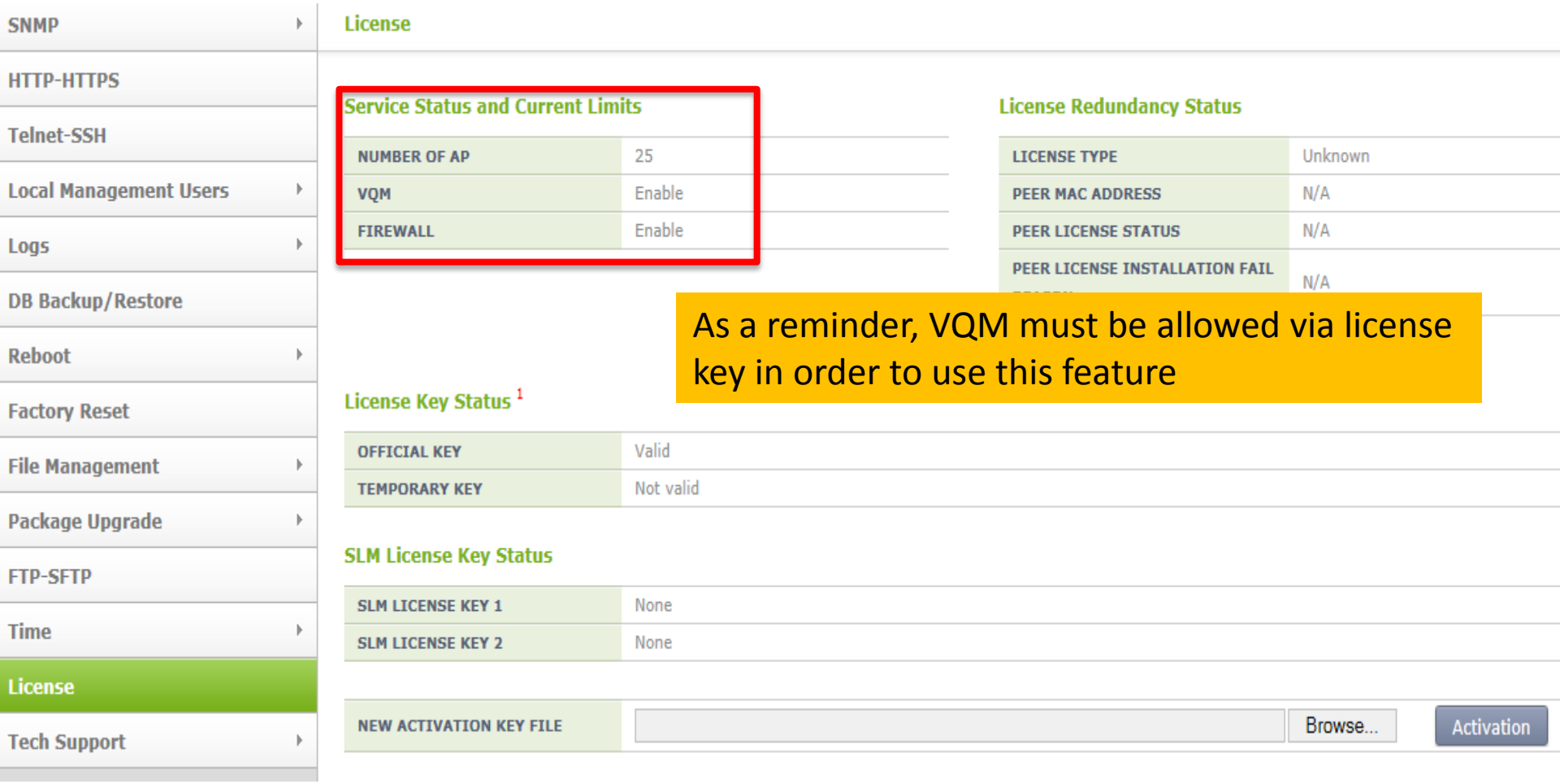
Samsung Wireless Enterprise™

Features

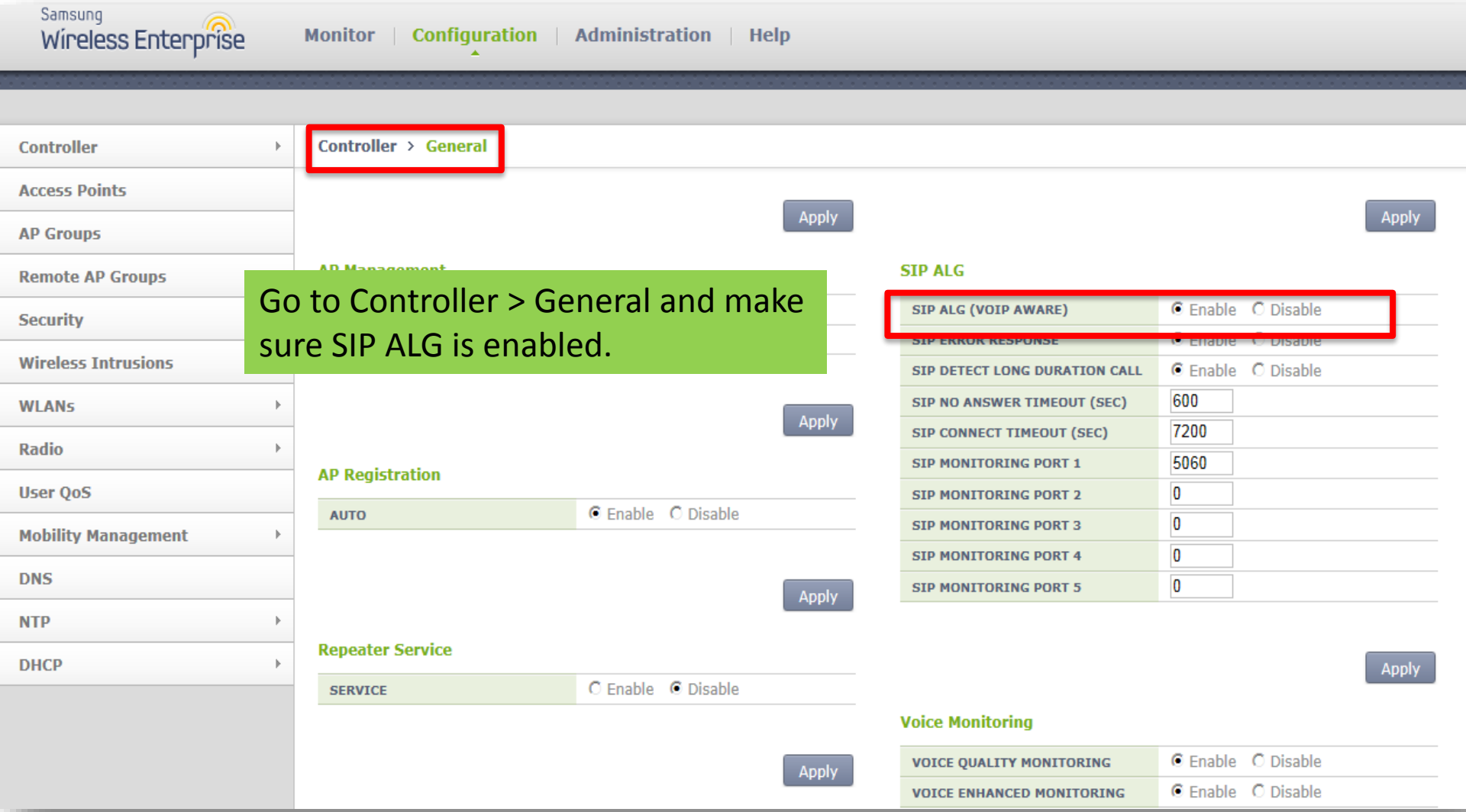
- Voice Call Signal Tracing and Troubleshooting
- Voice Quality Check
- Statistics related to Voice traffic

3.5.3 Configuration for VQM

Samsung Wireless Enterprise™

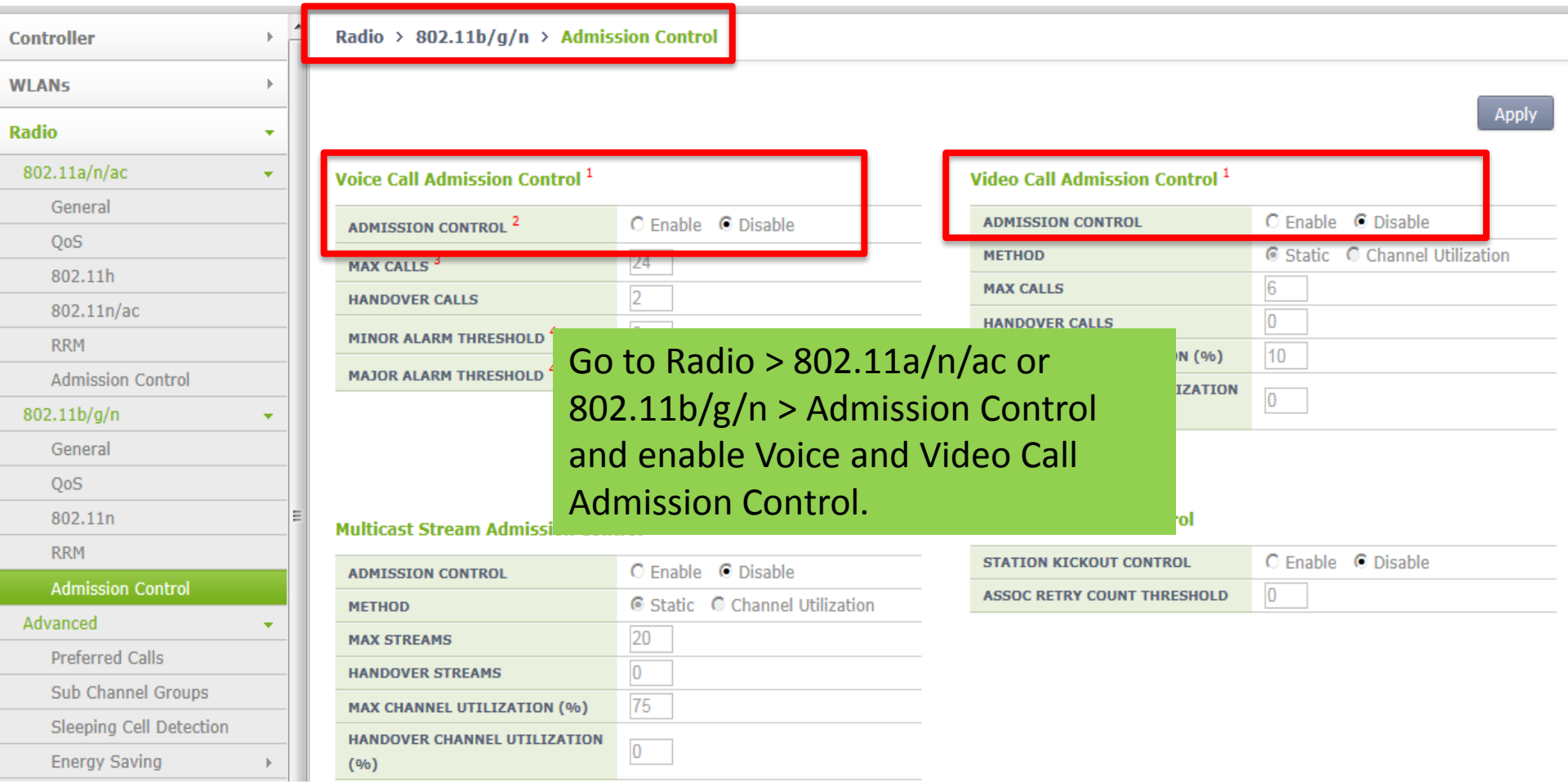


3.5.3 Configuration for VQM



Go to Controller > General and make sure SIP ALG is enabled.

3.5.3 Configuration for VQM

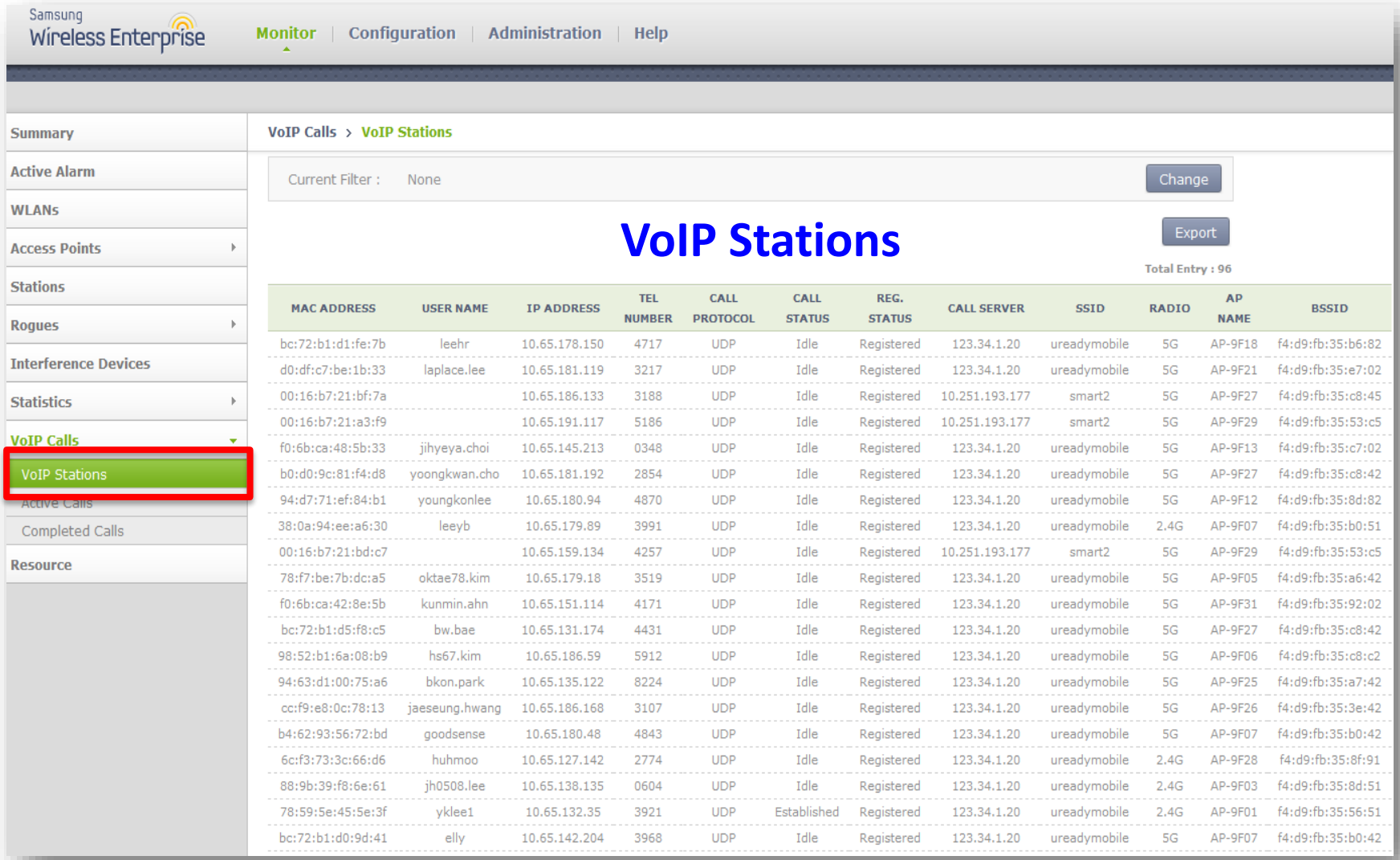


Samsung Wireless Enterprise™

3.5.4 Monitoring Voice Traffic

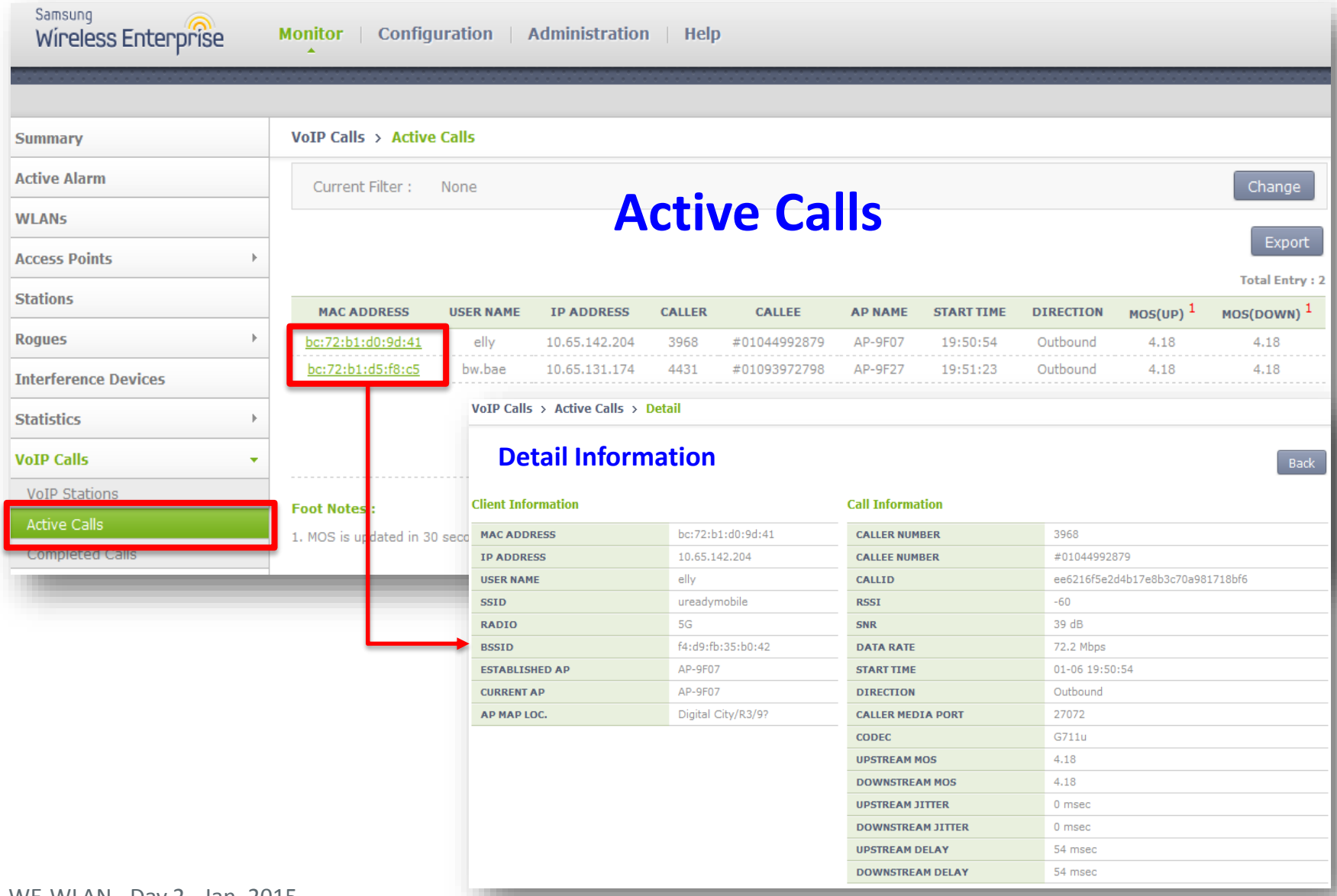
- 3.5.4.1 VoIP Calls
- 3.5.4.2 Statistics

3.5.4.1 VoIP Calls

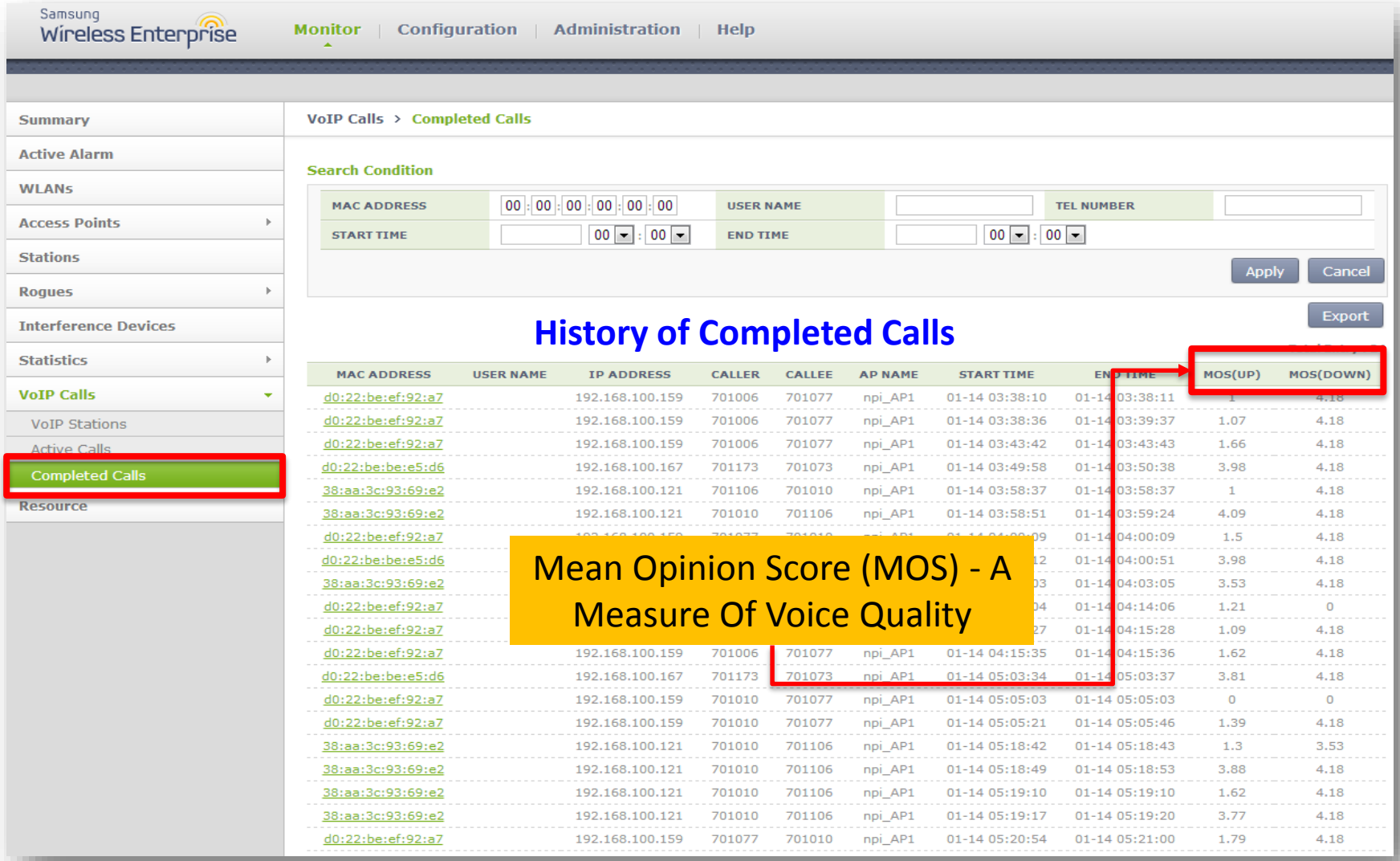


MAC ADDRESS	USER NAME	IP ADDRESS	TEL NUMBER	CALL PROTOCOL	CALL STATUS	REG. STATUS	CALL SERVER	SSID	RADIO	AP NAME	BSSID
bc:72:b1:d1:fe:7b	leehr	10.65.178.150	4717	UDP	Idle	Registered	123.34.1.20	ureadymobile	5G	AP-9F18	f4:d9:fb:35:b6:82
d0:df:c7:be:1b:33	laplace.lee	10.65.181.119	3217	UDP	Idle	Registered	123.34.1.20	ureadymobile	5G	AP-9F21	f4:d9:fb:35:e7:02
00:16:b7:21:bf:7a		10.65.186.133	3188	UDP	Idle	Registered	10.251.193.177	smart2	5G	AP-9F27	f4:d9:fb:35:c8:45
00:16:b7:21:a3:f9		10.65.191.117	5186	UDP	Idle	Registered	10.251.193.177	smart2	5G	AP-9F29	f4:d9:fb:35:53:c5
f0:6b:ca:48:5b:33	jihyeya.choi	10.65.145.213	0348	UDP	Idle	Registered	123.34.1.20	ureadymobile	5G	AP-9F13	f4:d9:fb:35:c7:02
b0:d0:9c:81:f4:d8	yoongkwan.cho	10.65.181.192	2854	UDP	Idle	Registered	123.34.1.20	ureadymobile	5G	AP-9F27	f4:d9:fb:35:c8:42
94:d7:71:ef:84:b1	youngkonlee	10.65.180.94	4870	UDP	Idle	Registered	123.34.1.20	ureadymobile	5G	AP-9F12	f4:d9:fb:35:8d:82
38:0a:94:ee:a6:30	leeyb	10.65.179.89	3991	UDP	Idle	Registered	123.34.1.20	ureadymobile	2.4G	AP-9F07	f4:d9:fb:35:b0:51
00:16:b7:21:bd:c7		10.65.159.134	4257	UDP	Idle	Registered	10.251.193.177	smart2	5G	AP-9F29	f4:d9:fb:35:53:c5
78:f7:be:7b:dc:a5	oktae78.kim	10.65.179.18	3519	UDP	Idle	Registered	123.34.1.20	ureadymobile	5G	AP-9F05	f4:d9:fb:35:a6:42
f0:6b:ca:42:8e:5b	kunmin.ahn	10.65.151.114	4171	UDP	Idle	Registered	123.34.1.20	ureadymobile	5G	AP-9F31	f4:d9:fb:35:92:02
bc:72:b1:d5:f8:c5	bw.bae	10.65.131.174	4431	UDP	Idle	Registered	123.34.1.20	ureadymobile	5G	AP-9F27	f4:d9:fb:35:c8:42
98:52:b1:6a:08:b9	hs67.kim	10.65.186.59	5912	UDP	Idle	Registered	123.34.1.20	ureadymobile	5G	AP-9F06	f4:d9:fb:35:c8:c2
94:63:d1:00:75:a6	bkon.park	10.65.135.122	8224	UDP	Idle	Registered	123.34.1.20	ureadymobile	5G	AP-9F25	f4:d9:fb:35:a7:42
cc:f9:e8:0c:78:13	jaeseung.hwang	10.65.186.168	3107	UDP	Idle	Registered	123.34.1.20	ureadymobile	5G	AP-9F26	f4:d9:fb:35:3e:42
b4:62:93:56:72:bd	goodsense	10.65.180.48	4843	UDP	Idle	Registered	123.34.1.20	ureadymobile	5G	AP-9F07	f4:d9:fb:35:b0:42
6c:f3:73:3c:66:d6	huhmoo	10.65.127.142	2774	UDP	Idle	Registered	123.34.1.20	ureadymobile	2.4G	AP-9F28	f4:d9:fb:35:8f:91
88:9b:39:f8:6e:61	jh0508.lee	10.65.138.135	0604	UDP	Idle	Registered	123.34.1.20	ureadymobile	2.4G	AP-9F03	f4:d9:fb:35:8d:51
78:59:5e:45:5e:3f	yklee1	10.65.132.35	3921	UDP	Established	Registered	123.34.1.20	ureadymobile	2.4G	AP-9F01	f4:d9:fb:35:56:51
bc:72:b1:d0:9d:41	elly	10.65.142.204	3968	UDP	Idle	Registered	123.34.1.20	ureadymobile	5G	AP-9F07	f4:d9:fb:35:b0:42

3.5.4.1 VoIP Calls

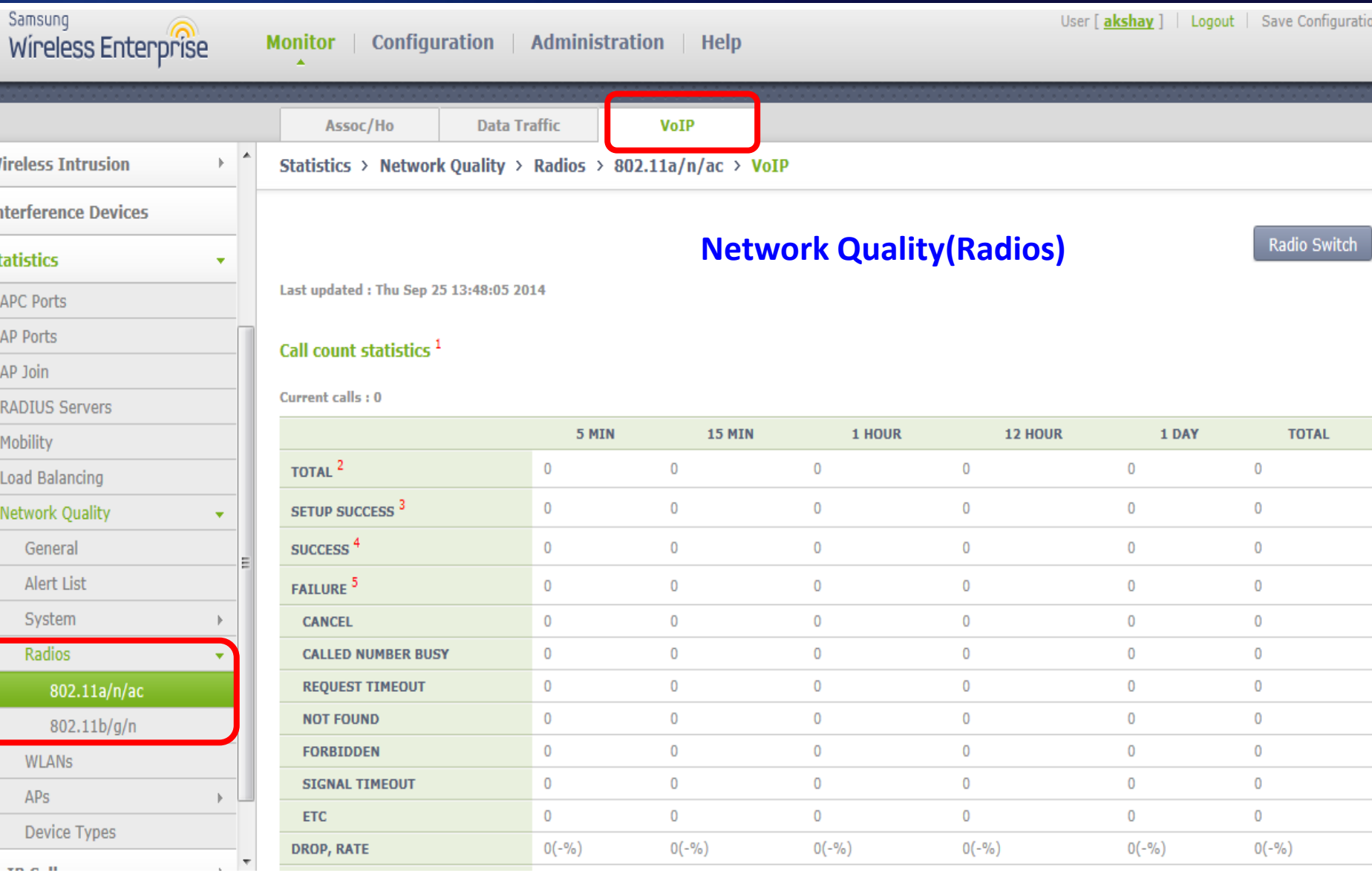


3.5.4.1 VoIP Calls

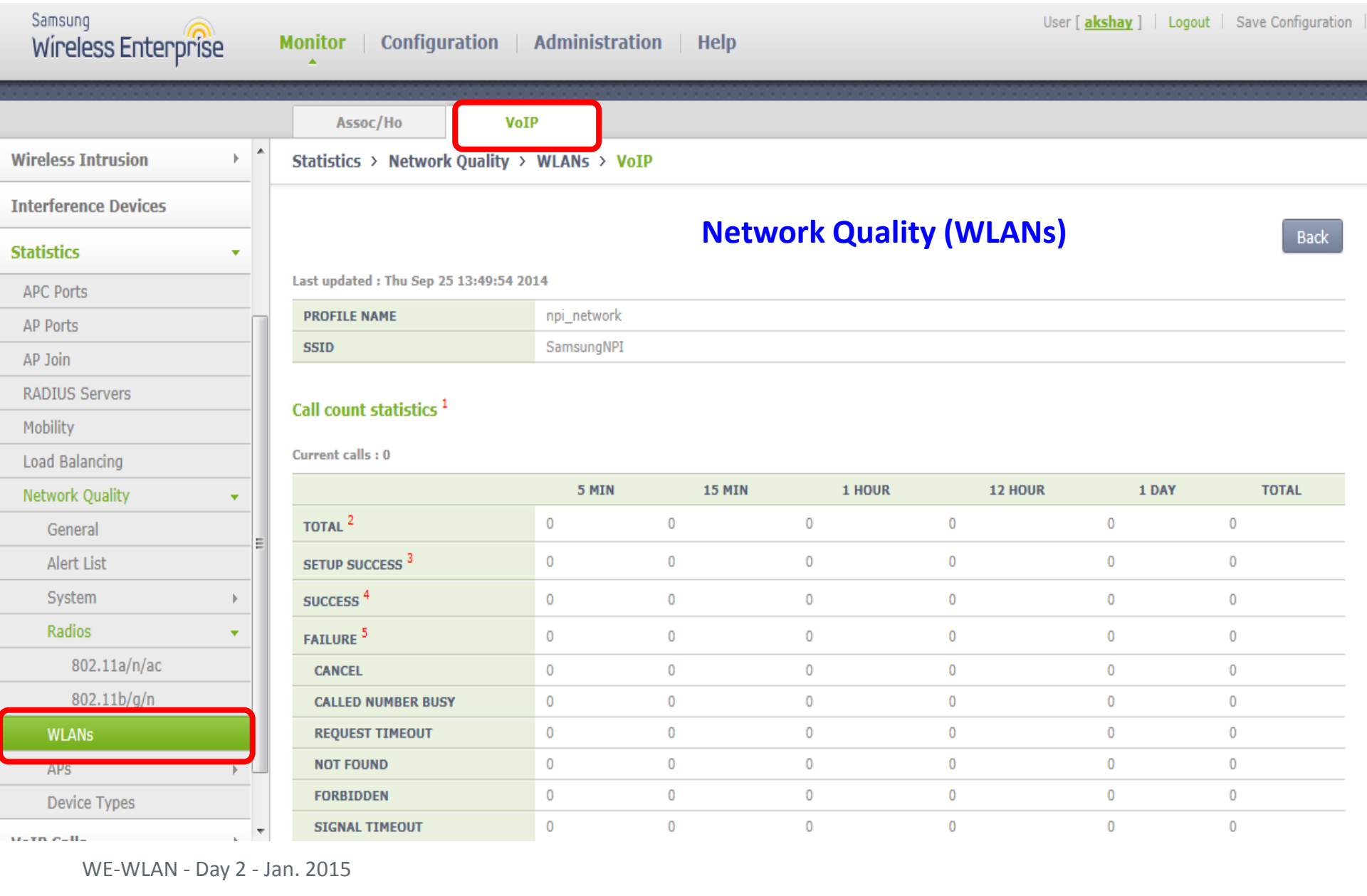


3.5.4.2 Statistics

Samsung Wireless Enterprise™

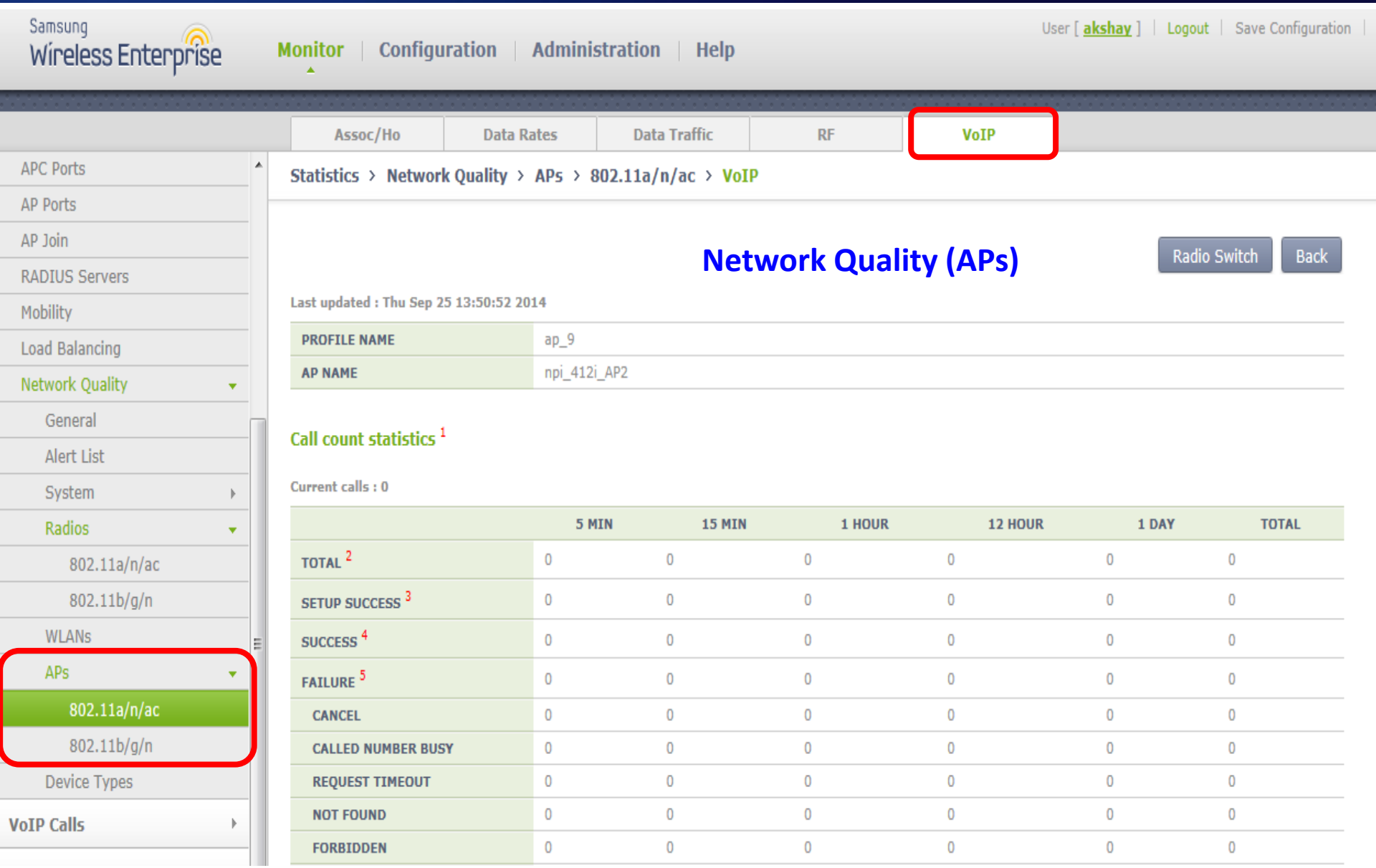


3.5.4.2 Statistics



3.5.4.2 Statistics

Samsung Wireless Enterprise™

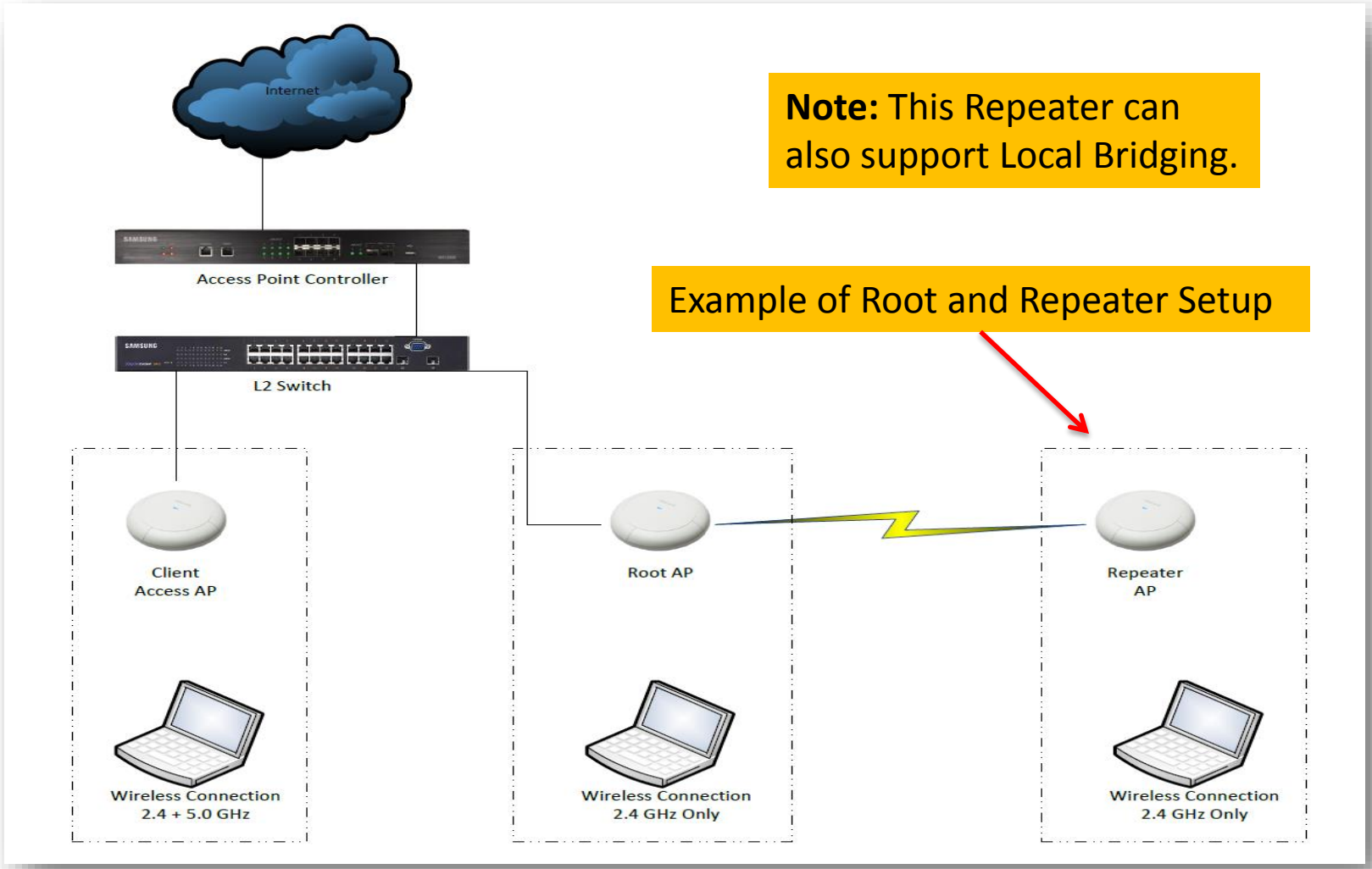


3.6 Root and Repeater AP

Samsung Wireless Enterprise™

- To provide a wireless LAN service where cable installation is difficult, a Samsung AP can be configured as a repeater mode to relay wireless LAN traffics.
- To configure this kind of network, the Repeater AP and Root AP are required.
- The Repeater AP is working as a wireless terminal and the Root AP connects a Repeater AP to a wireless terminal for connection to the WEC8500.
- The Root AP and Repeater AP will use radio 5GHz to connect to one another.
- Due to this, the Root and Repeater will only be able to broadcast its SSID on the 2.4Ghz radio

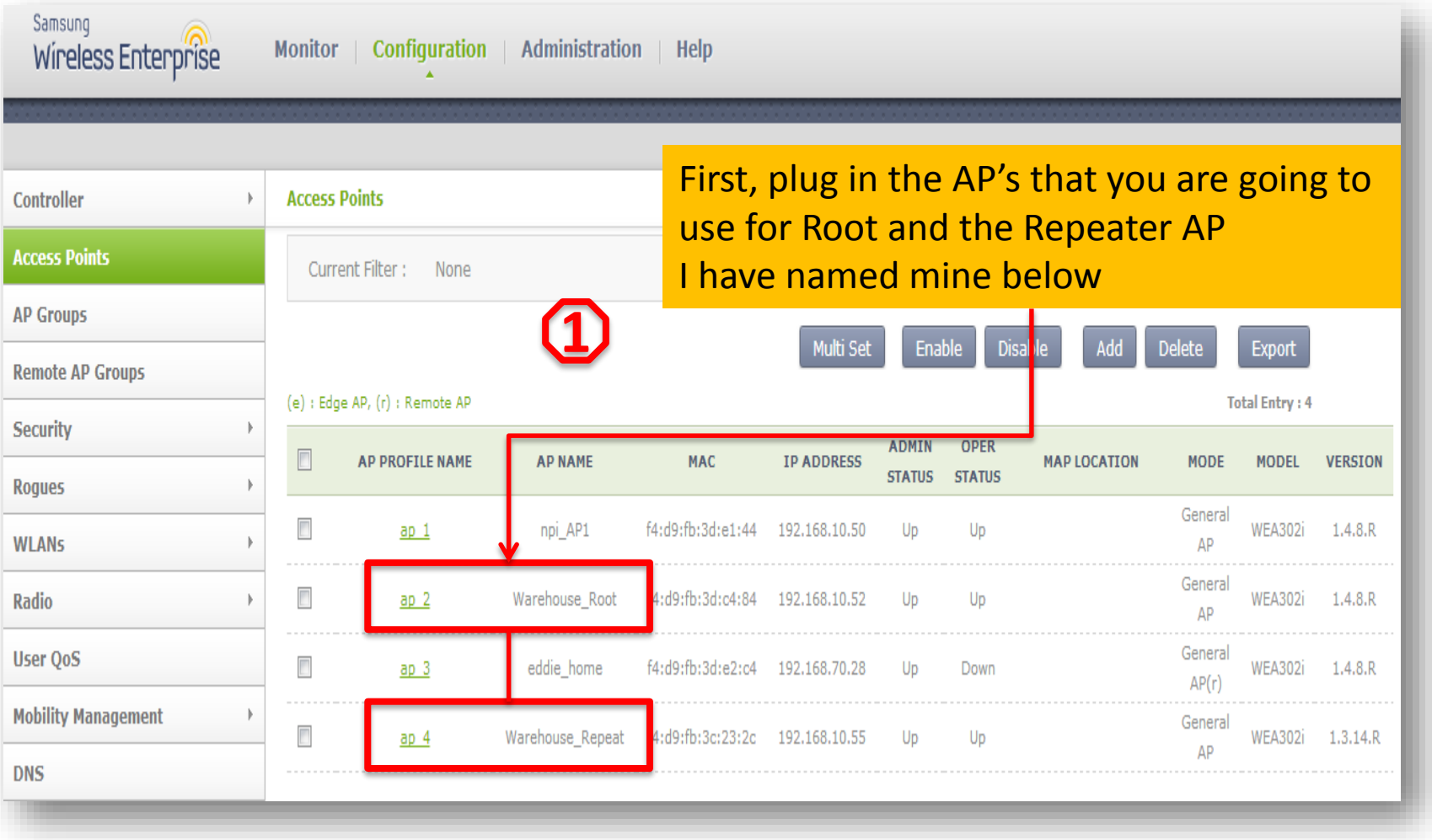
3.6 Root and Repeater AP



Note: This Repeater can also support Local Bridging.

Example of Root and Repeater Setup

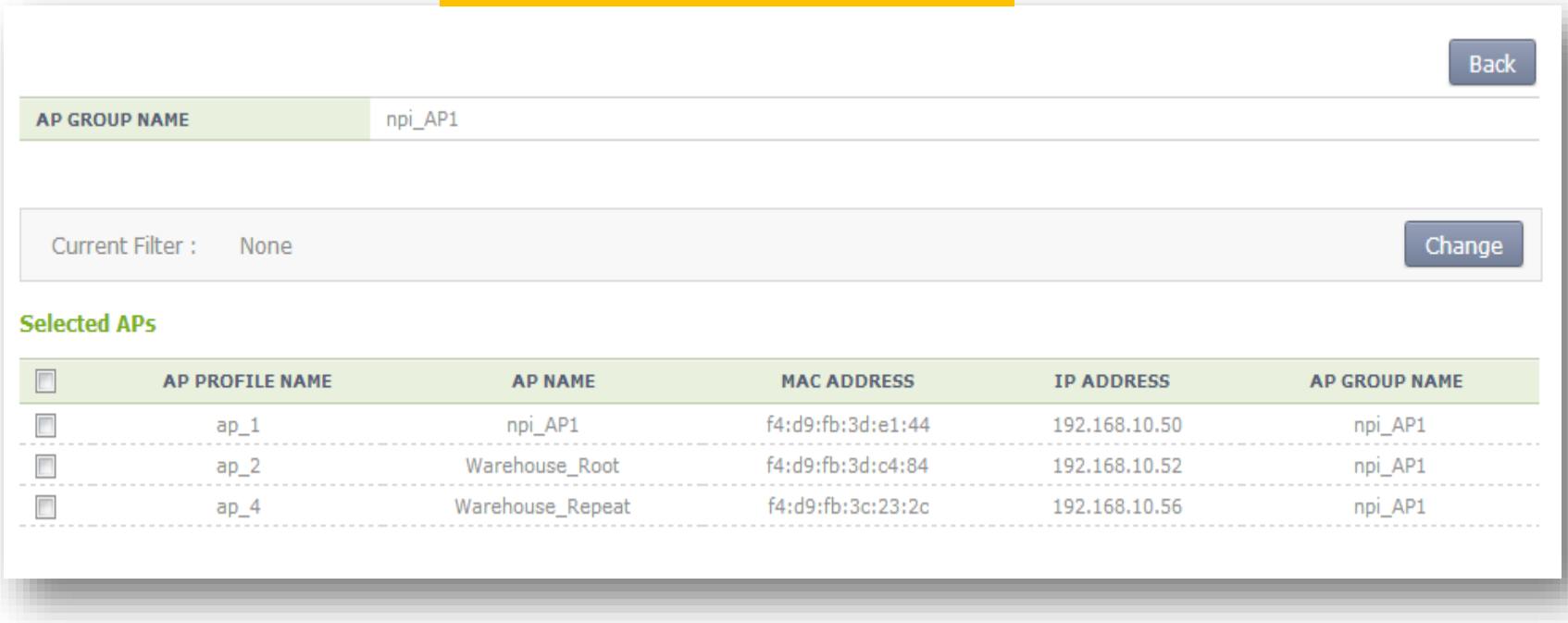
3.6 Root and Repeater AP



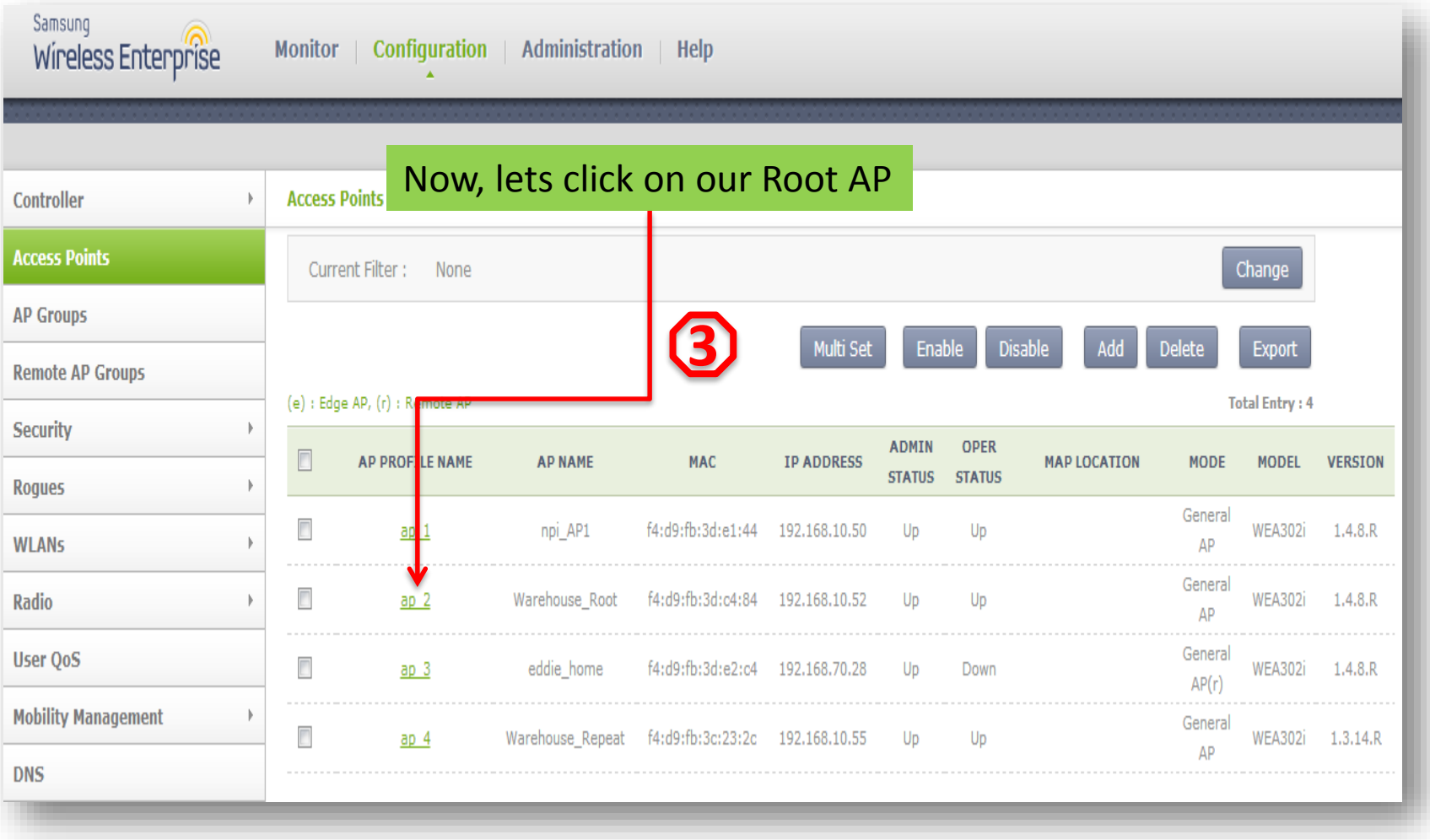
3.6 Root and Repeater AP

Samsung Wireless Enterprise™

The Root and Repeater AP's must be setup in the same AP Group.

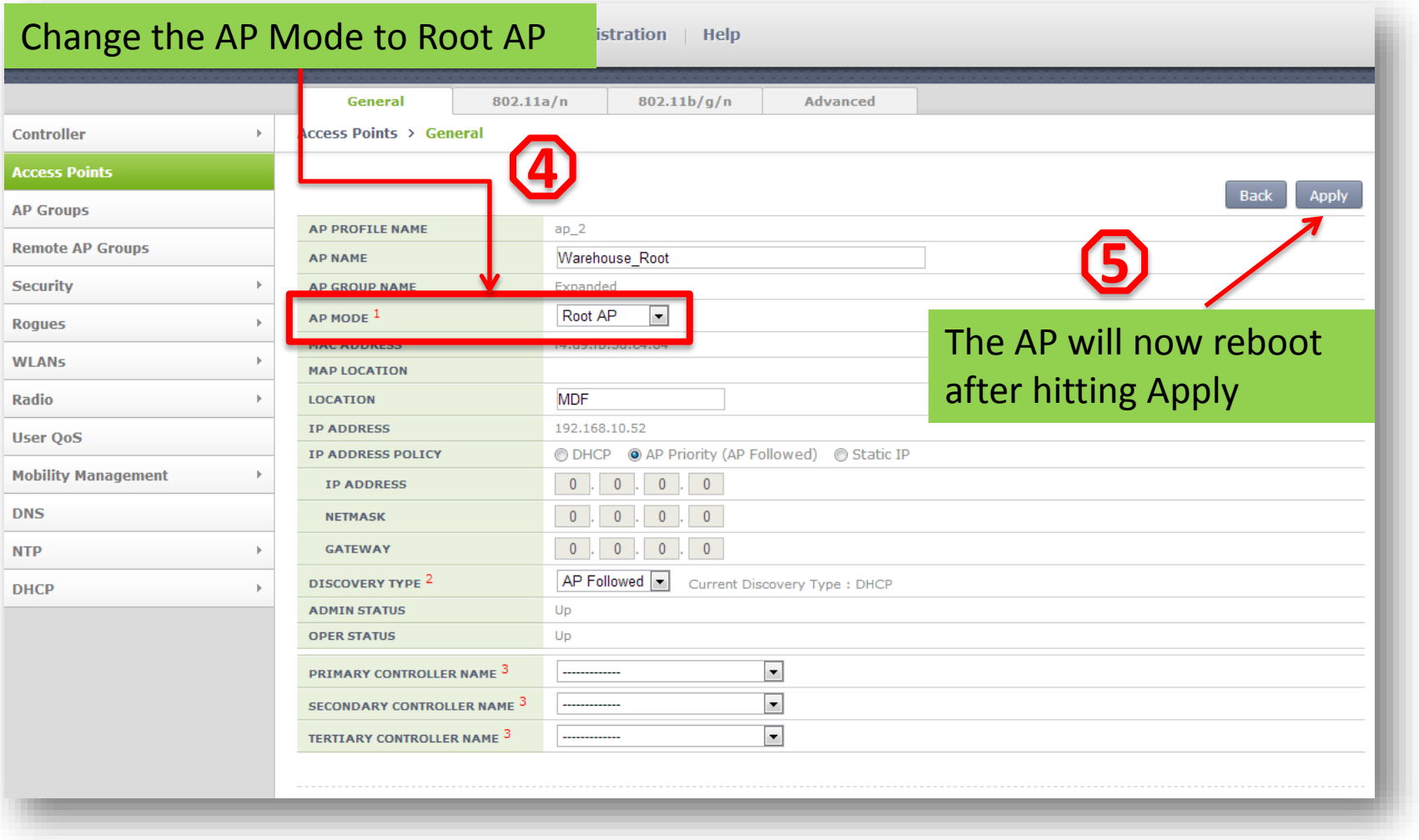


3.6 Root and Repeater AP

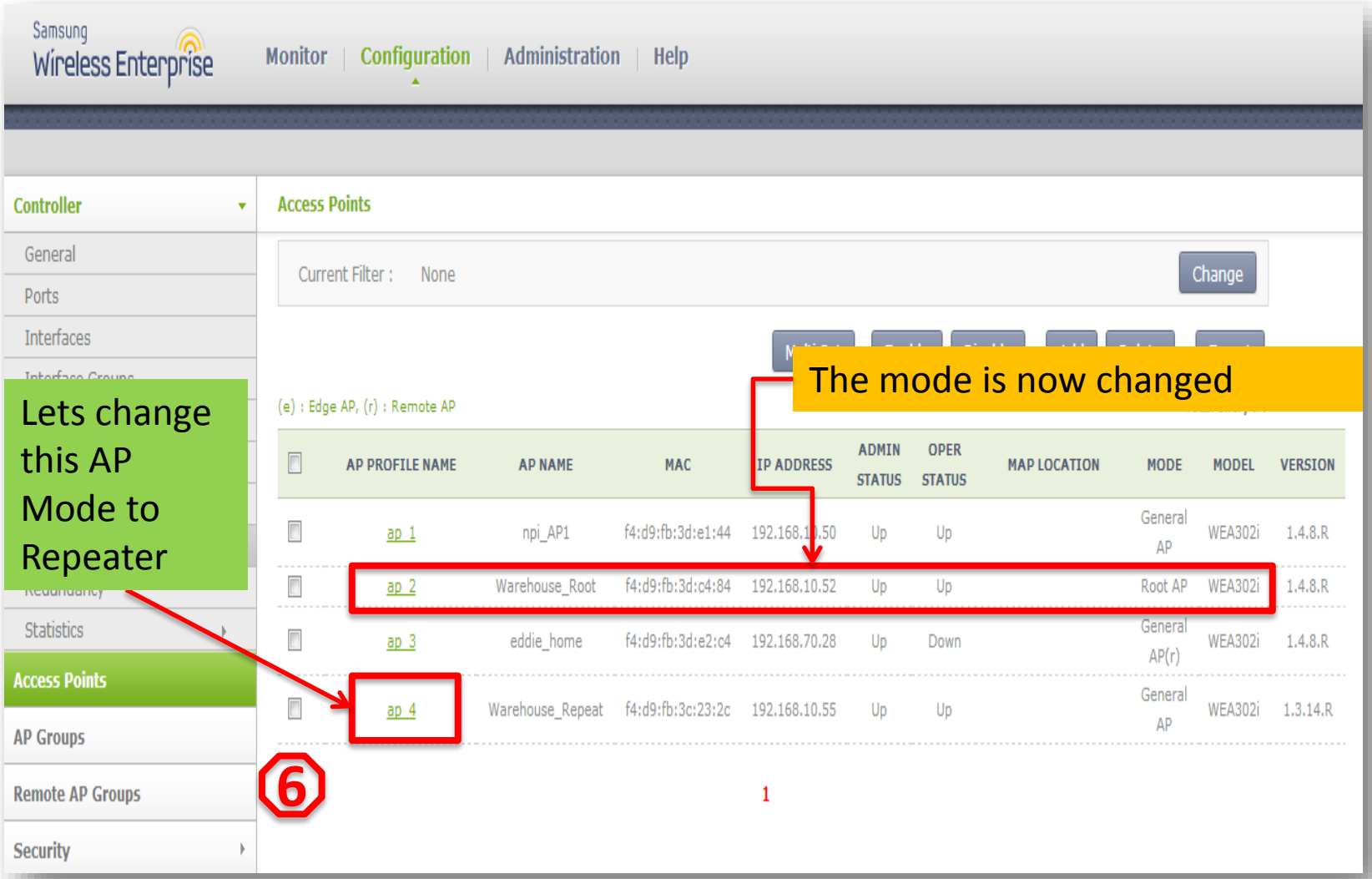


3.6 Root and Repeater AP

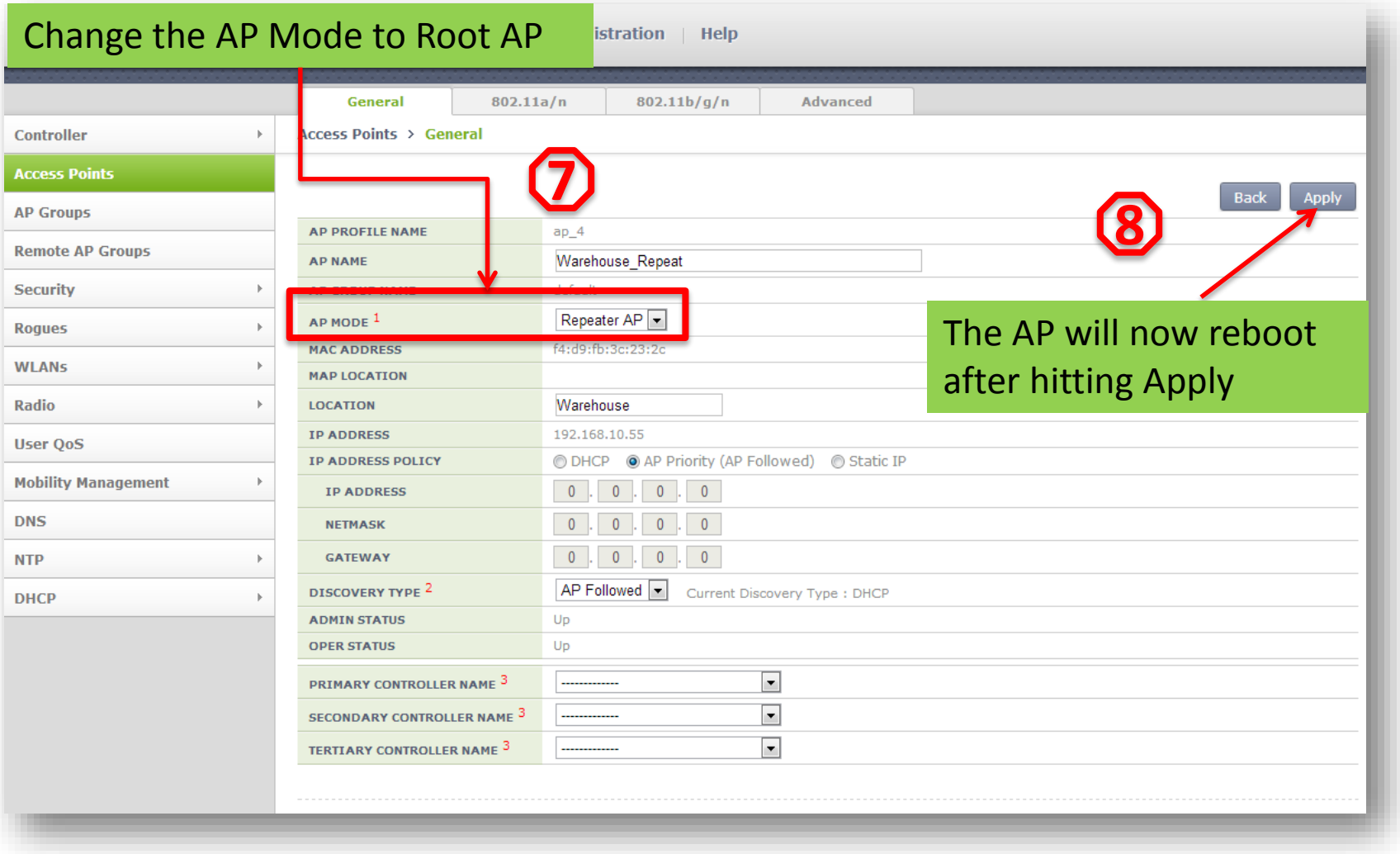
Samsung Wireless Enterprise™



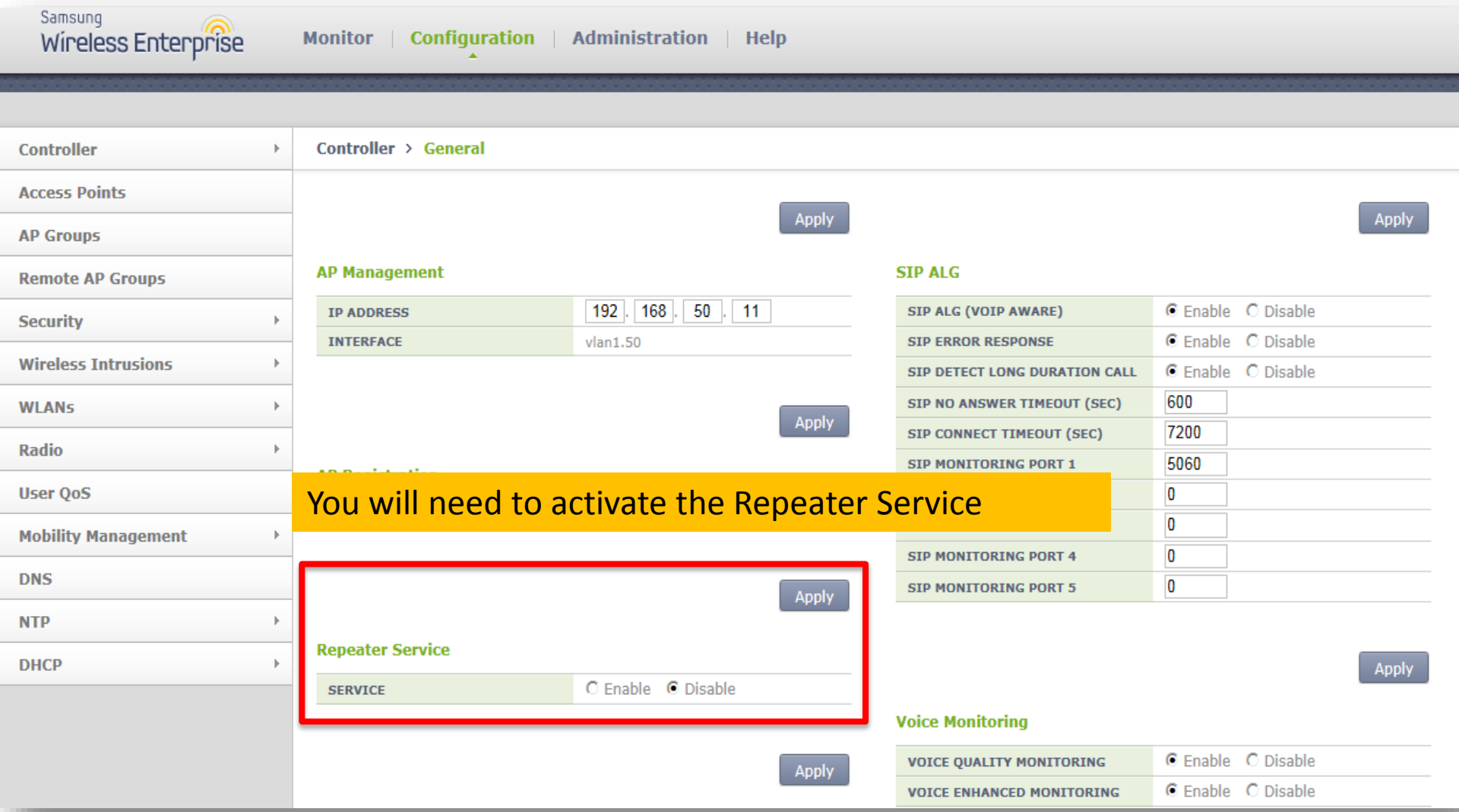
3.6 Root and Repeater AP



3.6 Root and Repeater AP



3.6 Root and Repeater AP



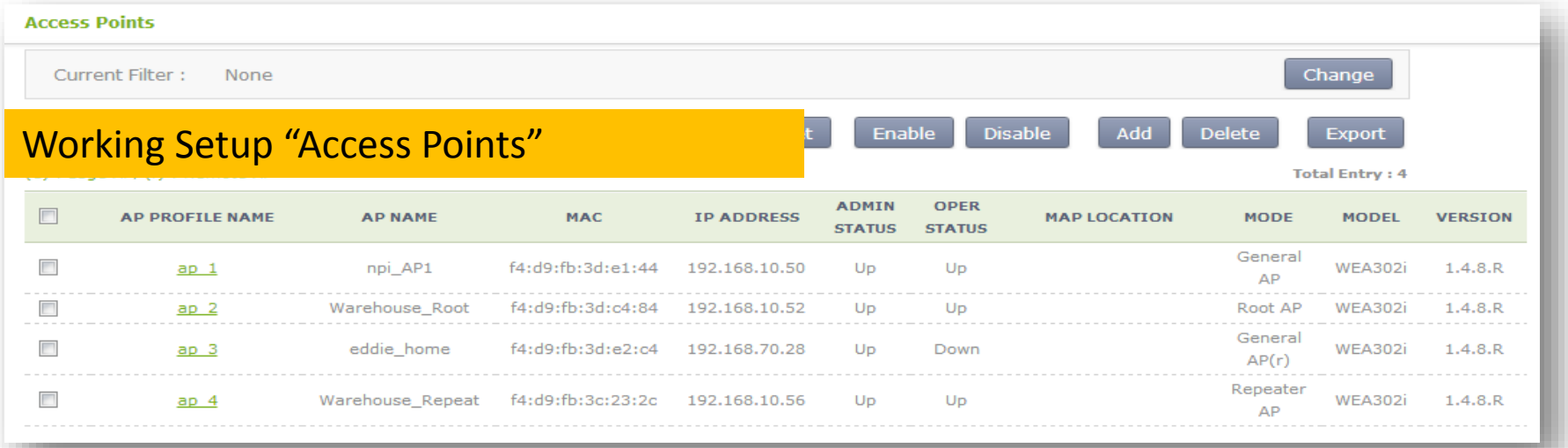
3.6 Root and Repeater AP

Samsung Wireless Enterprise™

- Now unplug the Repeater AP
- Install the Repeater AP with an external power supply
- The AP should now connect to the Root AP
- Once an AP has been changed to Root or Repeater type, it cannot be apart of the default AP Group.
- You must change the AP back to General or move the APs to another AP Group.

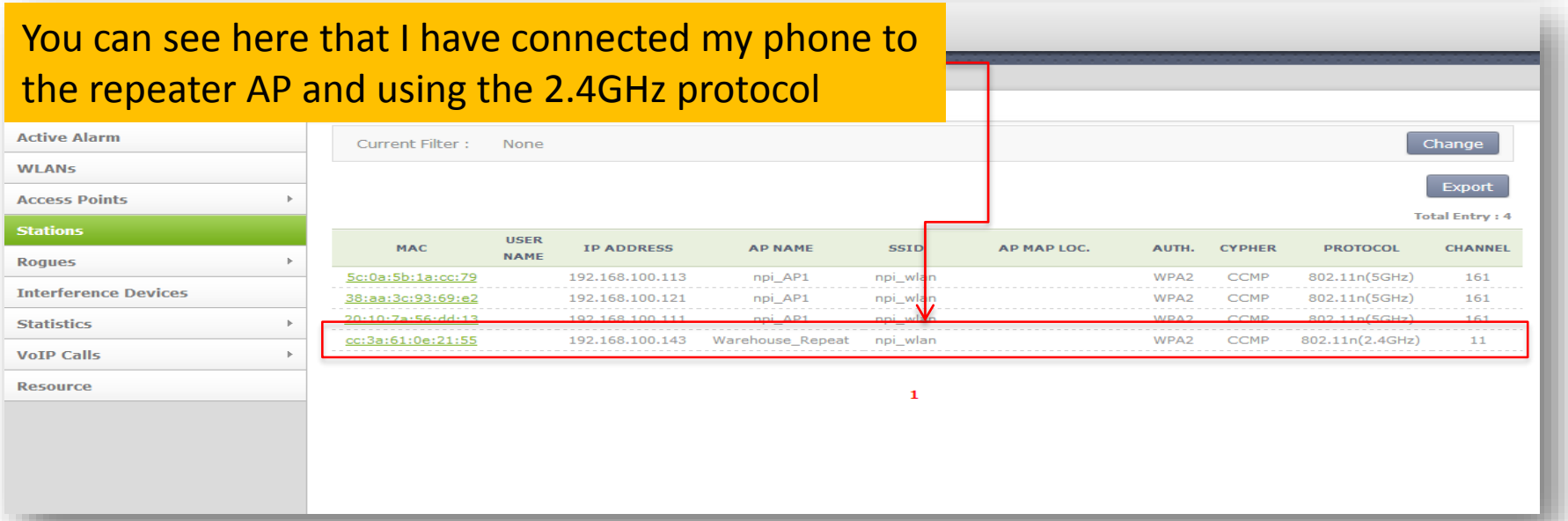
3.6 Root and Repeater AP

Samsung Wireless Enterprise™



Working Setup “Access Points”

You can see here that I have connected my phone to the repeater AP and using the 2.4GHz protocol



3.7 SNMP

Samsung Wireless Enterprise™

3.7 Simple Network Management Protocol (SNMP)

- 3.7.1 SNMP Supported
- 3.7.2 Enabling SNMP
- 3.7.3 Trap Control

3.7.1 SNMP Supported

Samsung Wireless Enterprise™

SNMP versions supported by Samsung APC

- SNMPv1/v2c : Community-based Simple Network Management Protocol Version 2
- SNMPv3 : Security model including authentication, encryption

Security Features in SNMPv2c/v3

Version	Level	Authentication	Encryption	How to work
v1/v2c	noAuthNoPriv	Community String	No	Uses a community string match for authentication
v3	noAuthNoPirv	Username	No	Uses a Username match for authentication
v3	authNoPriv	MD5 or SHA	No	Authentication based on the HMAC-MD5 or HMAC-SHA
v3	authPriv	MD5 or SHA	DES or AES	Encryption in addition to authentication based on the DES or AES

Trap

- SNMP Trap can be configured on the both WEC and CLI.

Notice

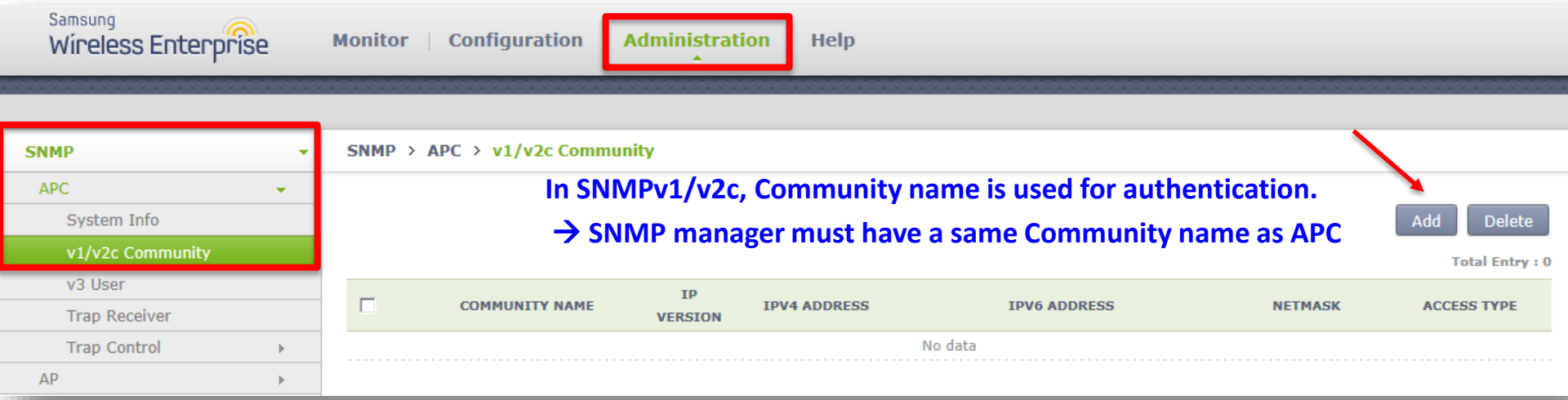
- SNMPv1/v2c and v3 can be configured on the both WEC and CLI modes
- Each AP does not support SNMP agent.
- Typically, SNMP set/get packet use port 161, SNMP Trap/inform packet use port 162.
- Port number of SNMP Trap/inform is configurable.

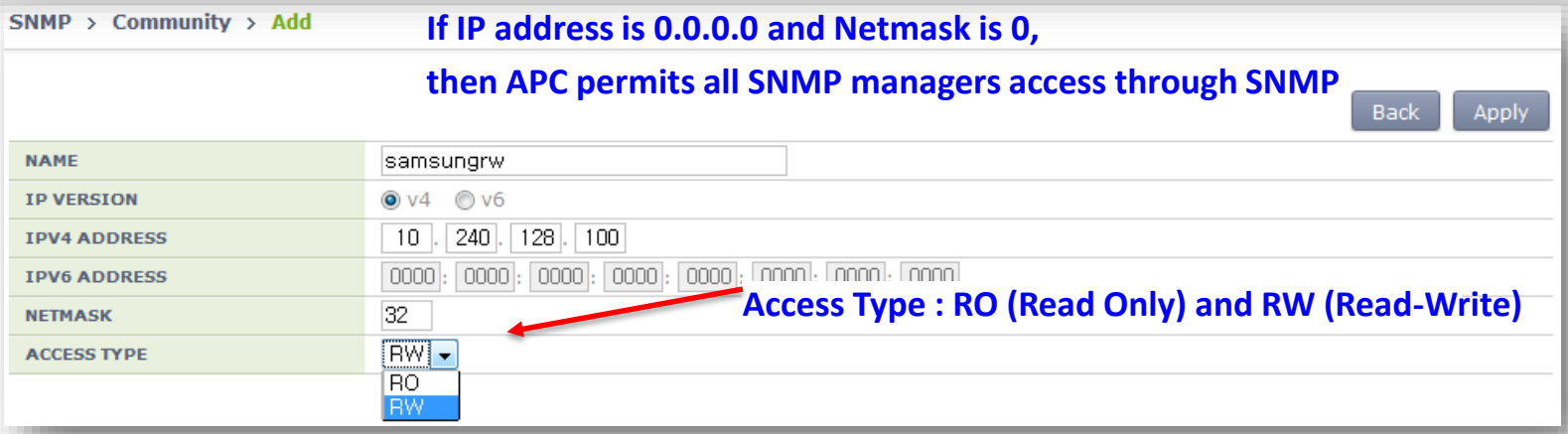
Samsung Wireless Enterprise™

3.7.2 Enabling SNMP

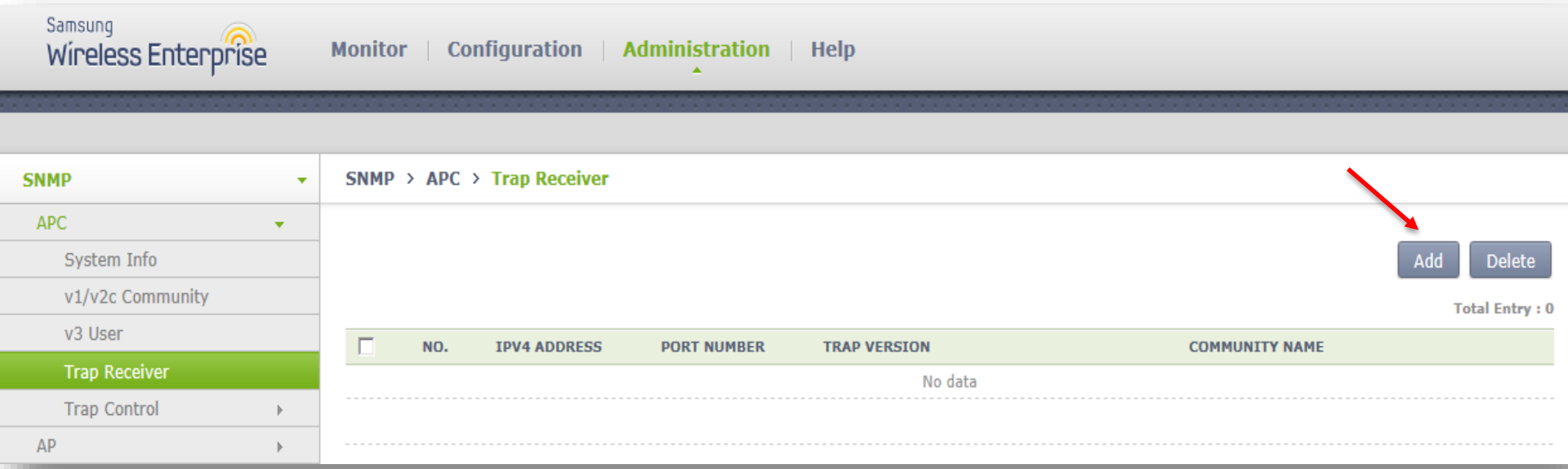
- 3.7.2.1 SNMP v1/v2c
- 3.7.2.2 SNMPv3

3.7.2.1 SNMP v1/v2c

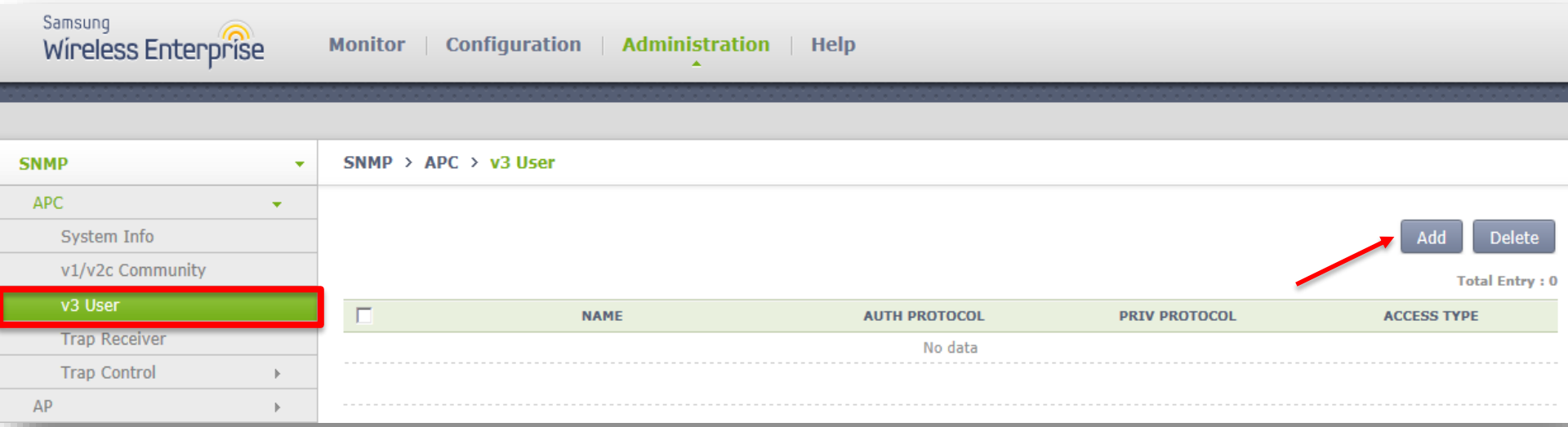


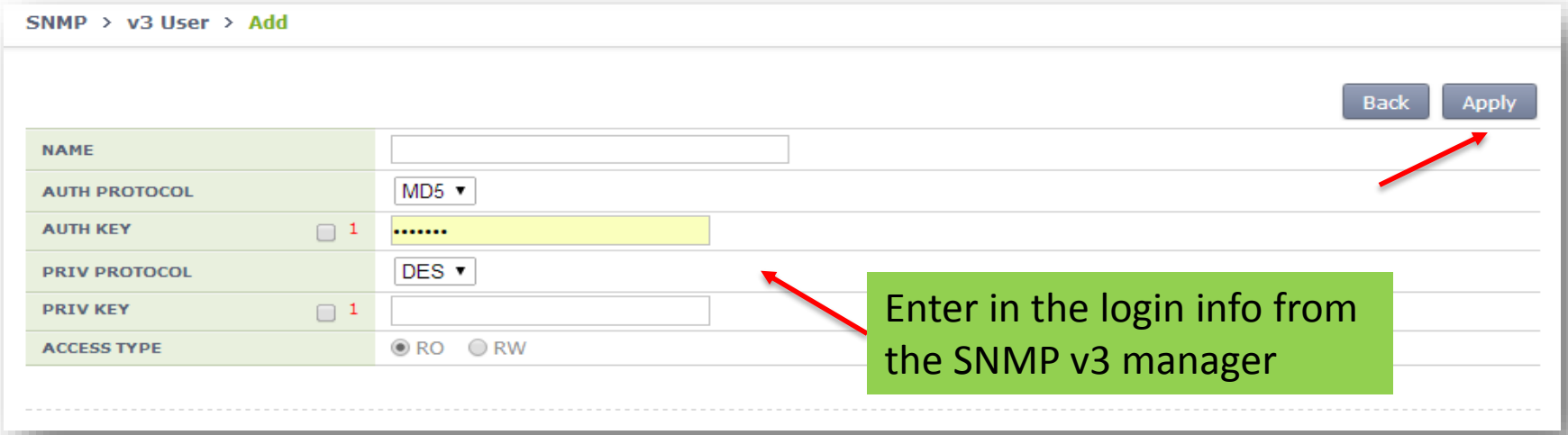


3.7.2.1 SNMP v1/v2c



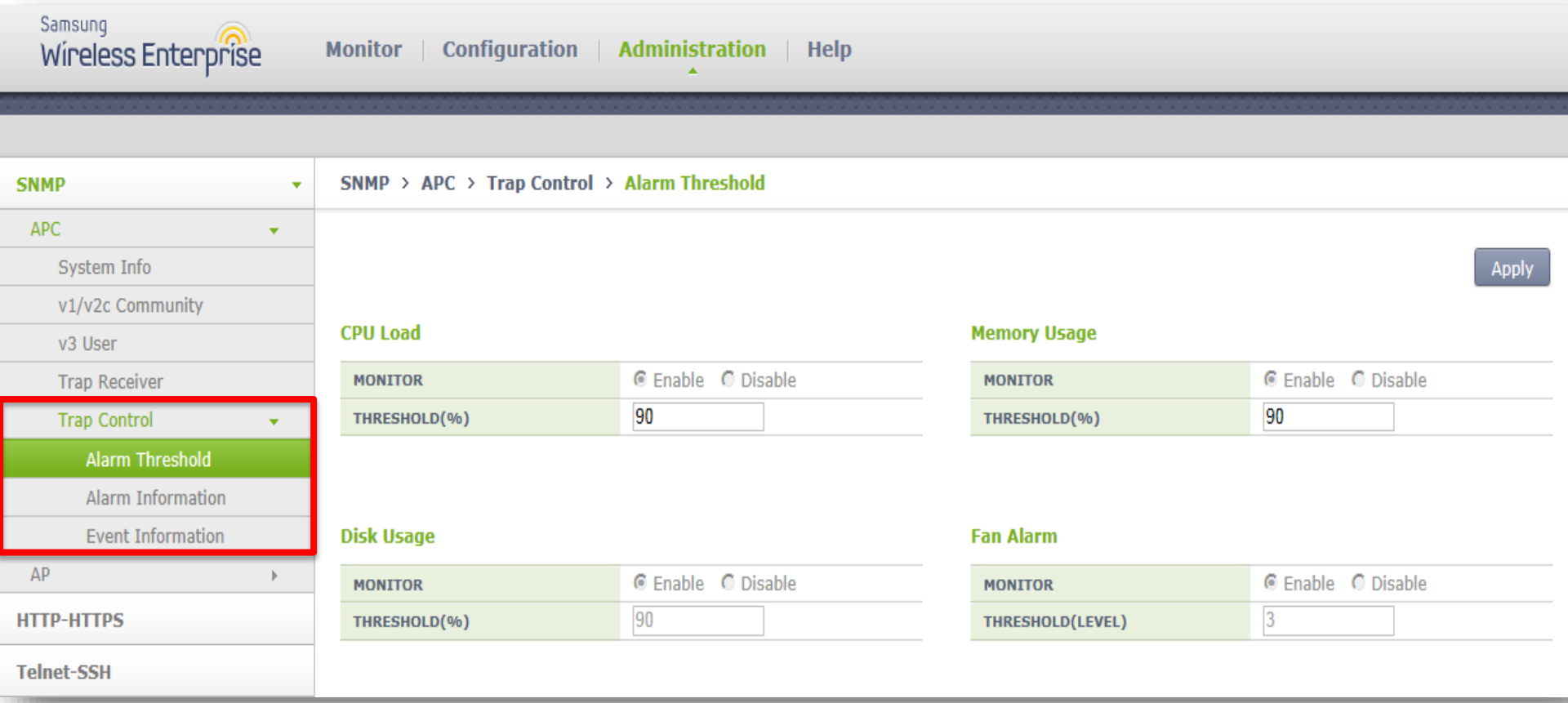
3.7.2.2 SNMPv3


Samsung Wireless Enterprise
Monitor
Configuration
Administration
Help
SNMP
APC
System Info
v1/v2c Community
v3 User
Trap Receiver
Trap Control
AP
SNMP > APC > v3 User
Add
Delete
Total Entry : 0
NAME
AUTH PROTOCOL
PRIV PROTOCOL
ACCESS TYPE
No data


SNMP > v3 User > Add
Back
Apply
NAME
AUTH PROTOCOL
MD5
AUTH KEY
PRIV PROTOCOL
DES
PRIV KEY
ACCESS TYPE
RO
RW
Enter in the login info from the SNMP v3 manager

3.7.3 Trap Control

Here you can set the alarm thresholds

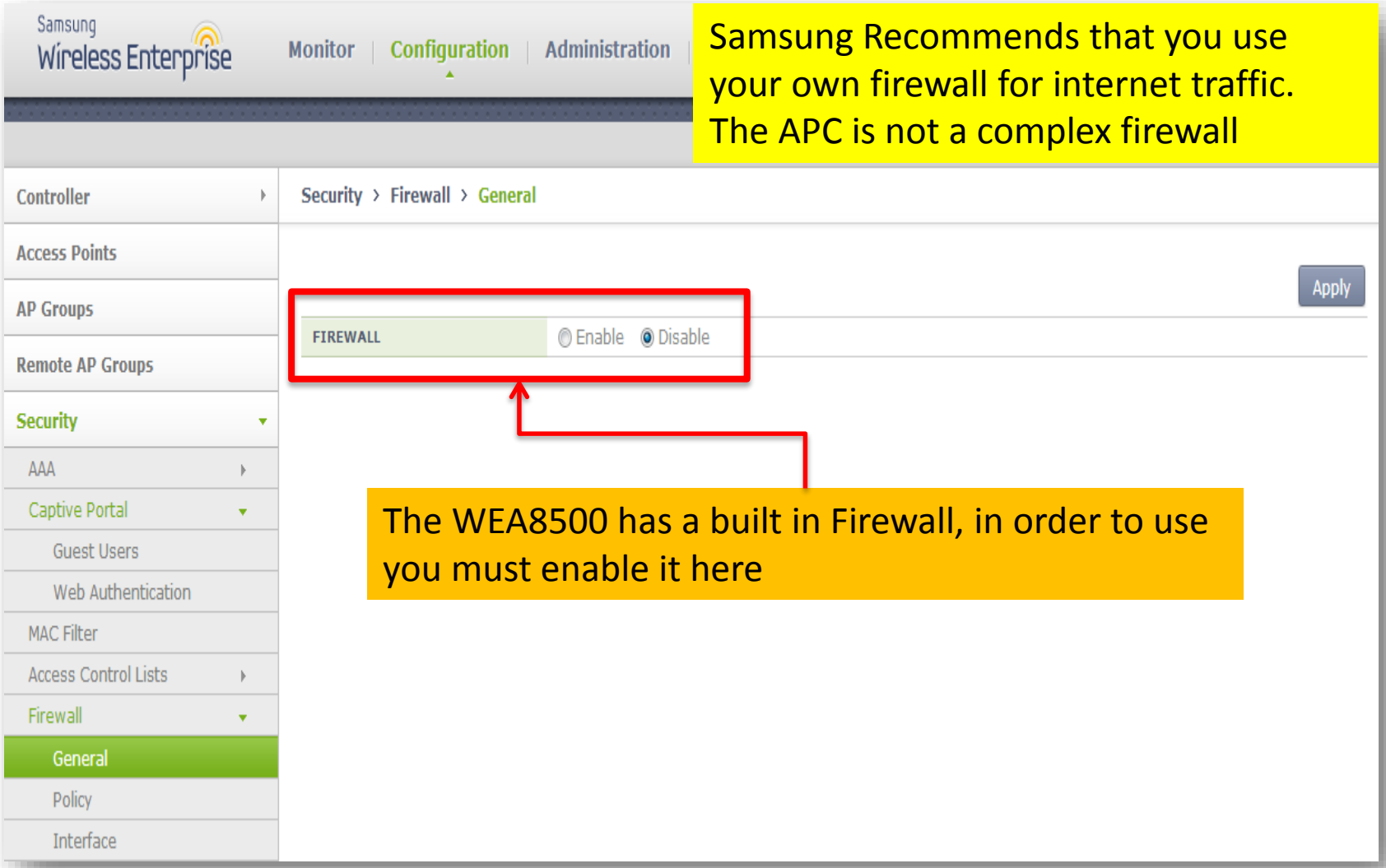


Samsung Wireless Enterprise™

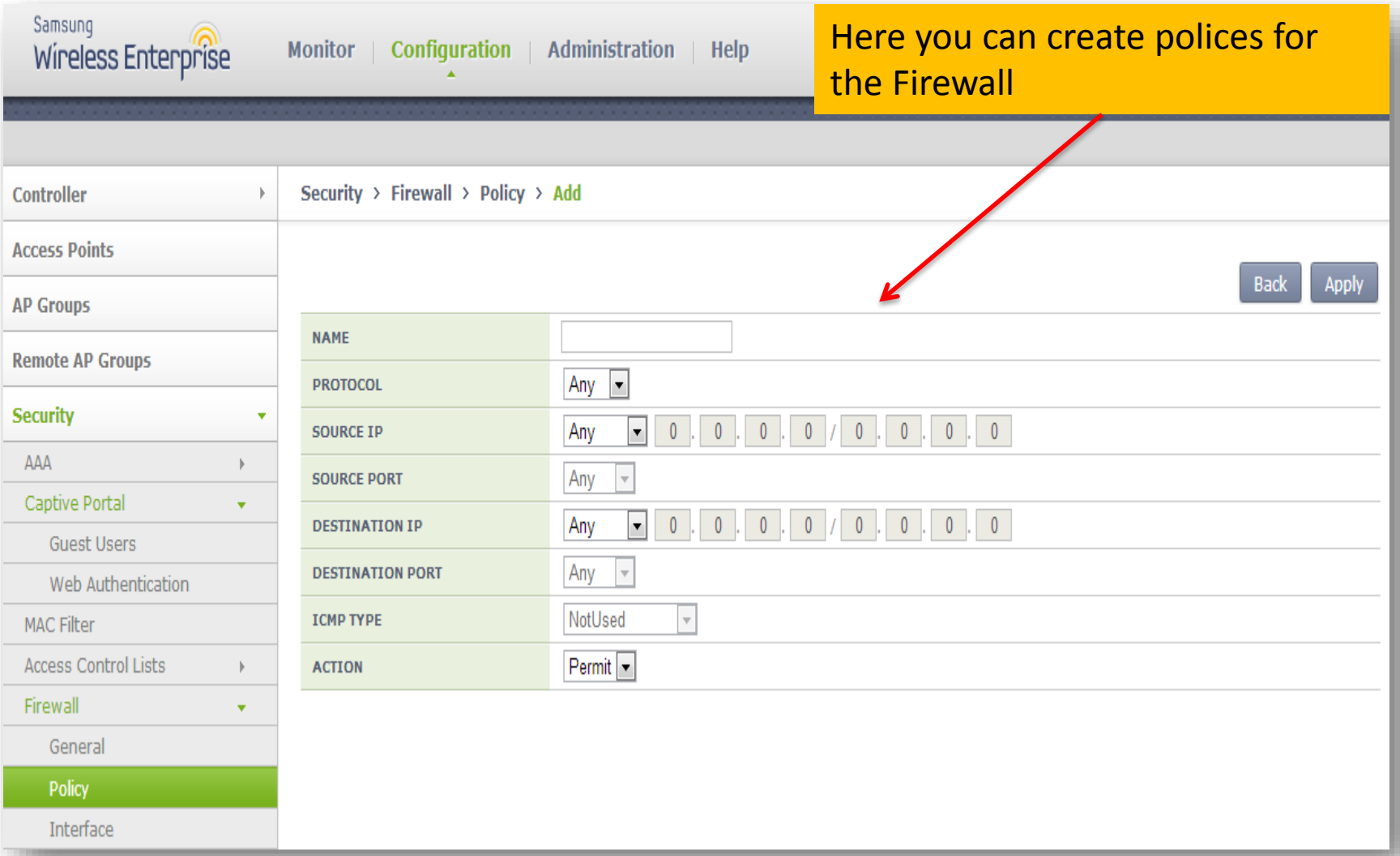
4. Security

- 4.1 Firewall / ACL
- 4.2 Captive Portal
- 4.3 Web Pass-Through
- 4.4 Conditional Web Redirection

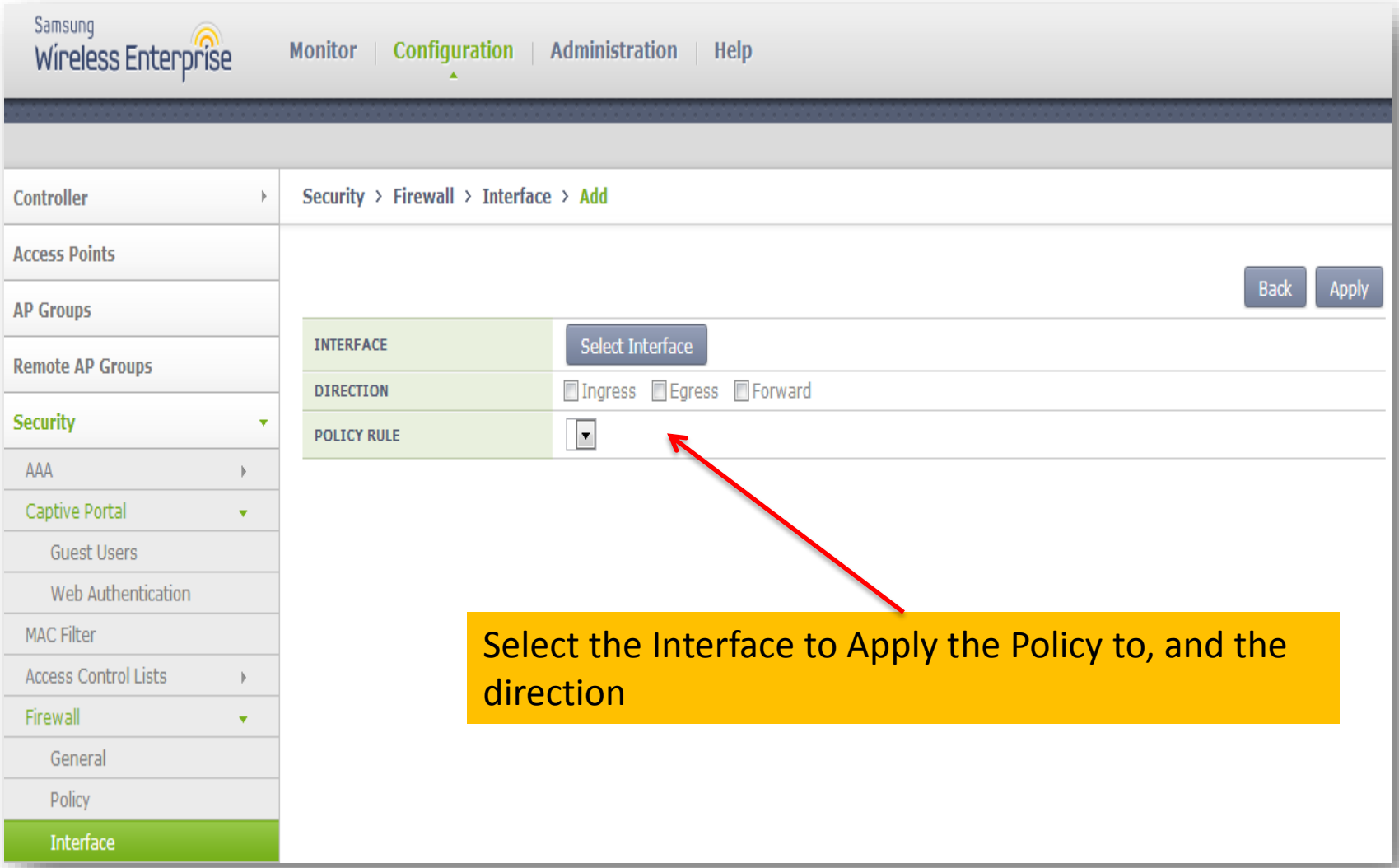
4.1 Firewall / ACL



4.1 Firewall / ACL



4.1 Firewall / ACL



Samsung Wireless Enterprise™

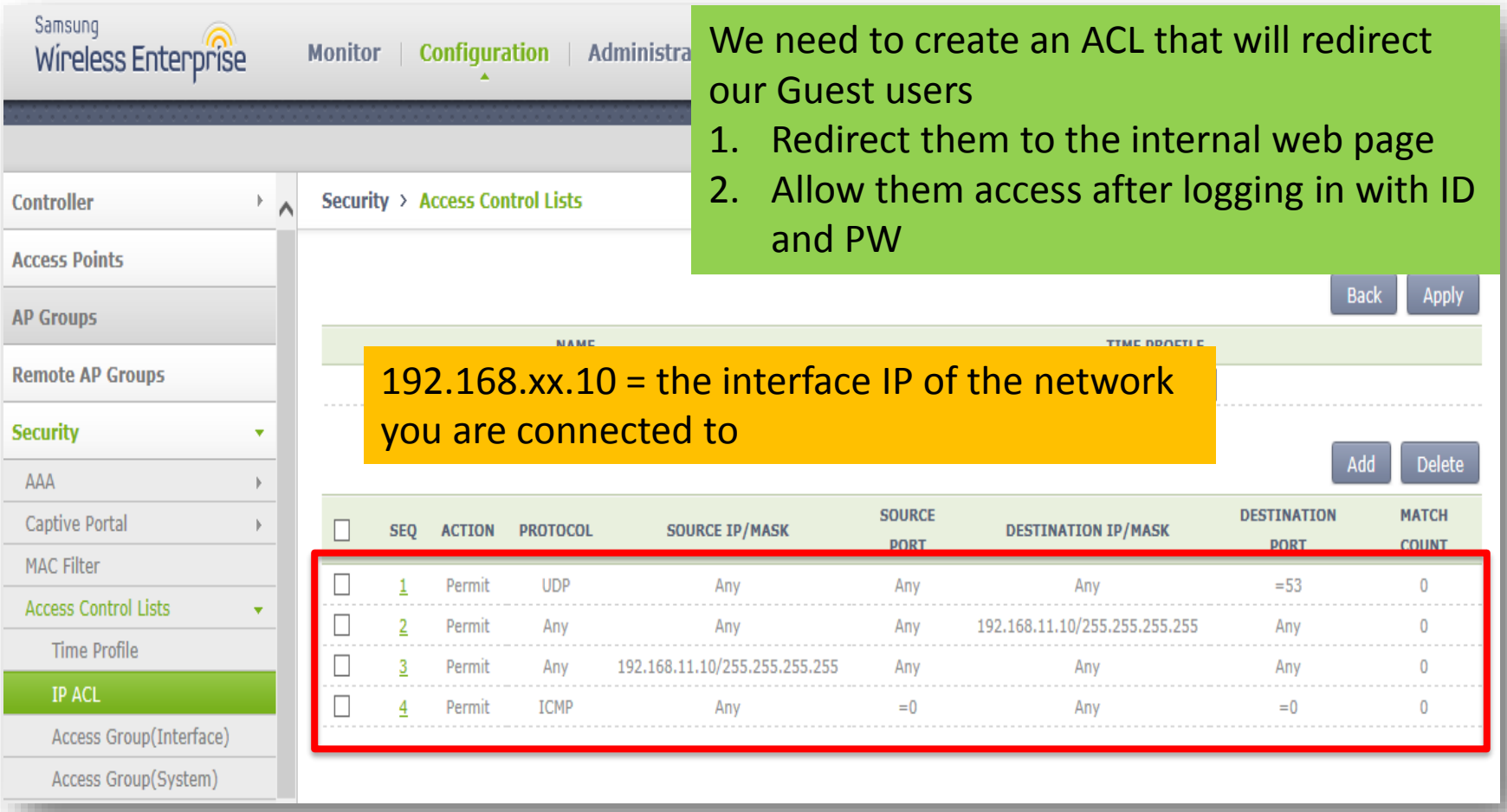
4.2 Captive Portal

- 4.2.1 Introduction
- 4.2.2 Access Control List
- 4.2.3 Guest Access WLAN
- 4.2.4 Web Authentication
- 4.2.4 Guest Users
- 4.2.5 Lobby Ambassador
- 4.2.6 Enable WLAN

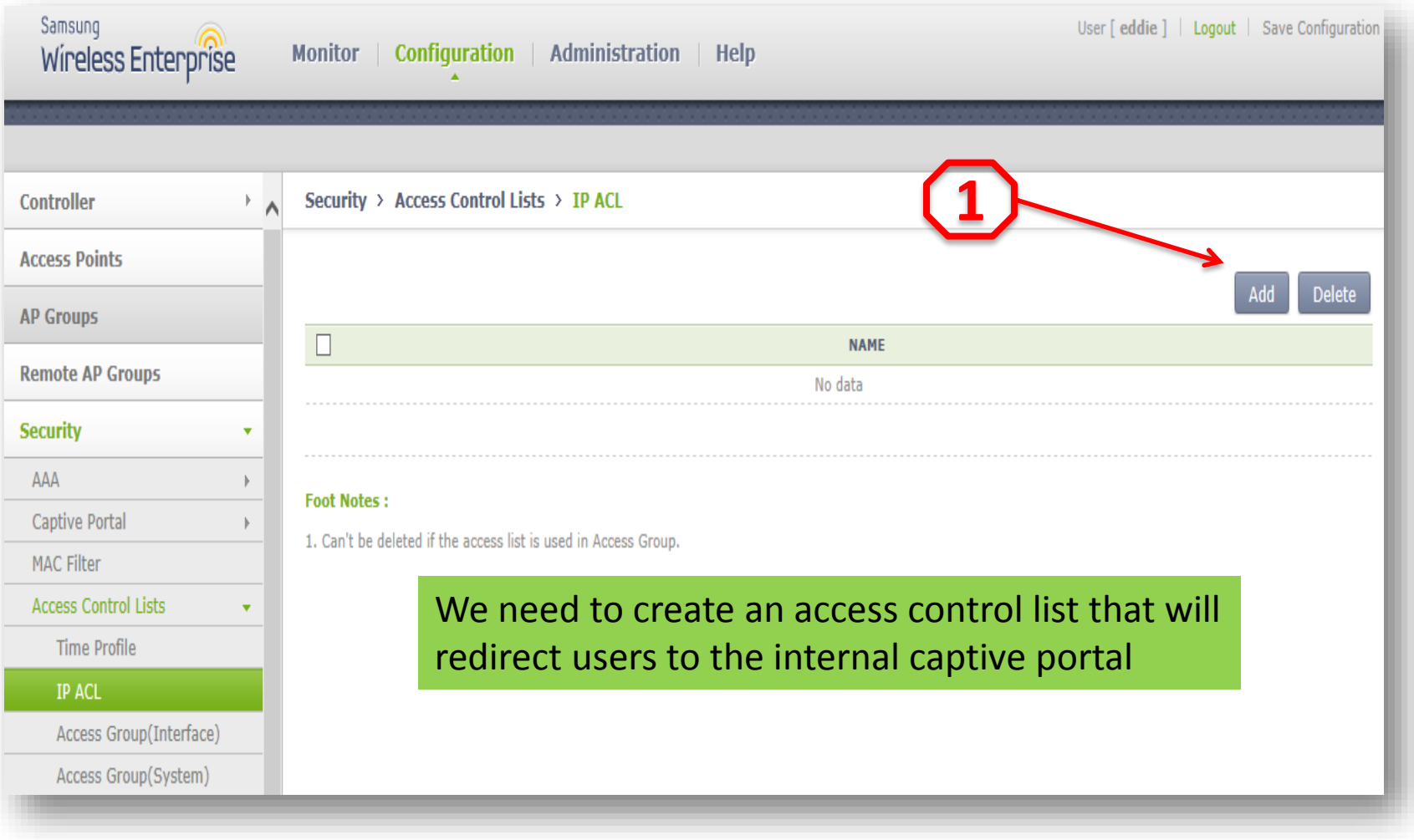
4.2.1 Introduction

- Samsung's wireless LAN system provides a built-in Guest Access function.
- A guest will be granted limited service after connecting to a specific WLAN (SSID).
- The Guest will be redirected to a login page, where at the time they must enter the ID and Password provided by the WLAN administrator or the Lobby Ambassador.
- This will gain the Guest access to the network

4.2.2 Access Control List

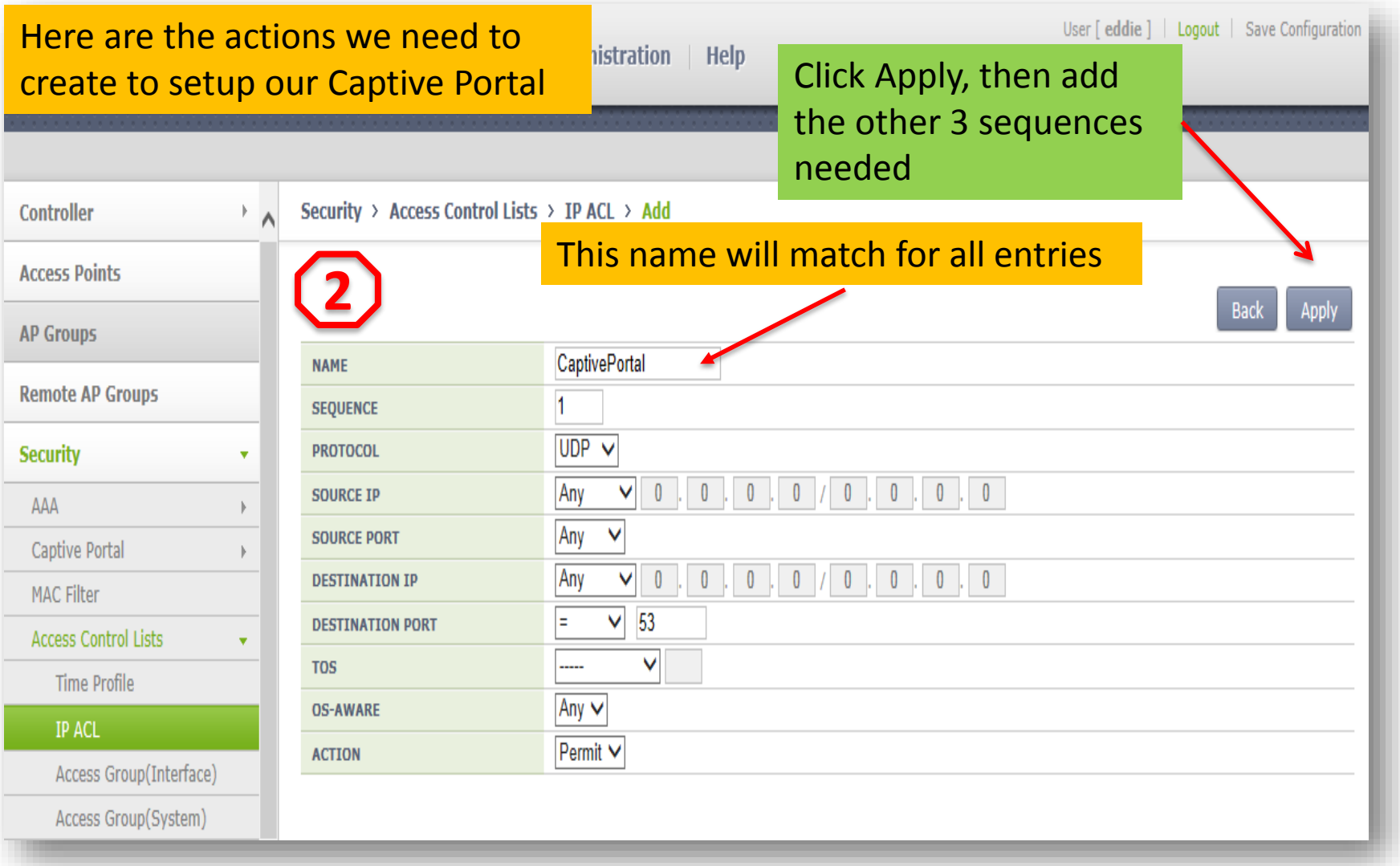


4.2.2 Access Control List

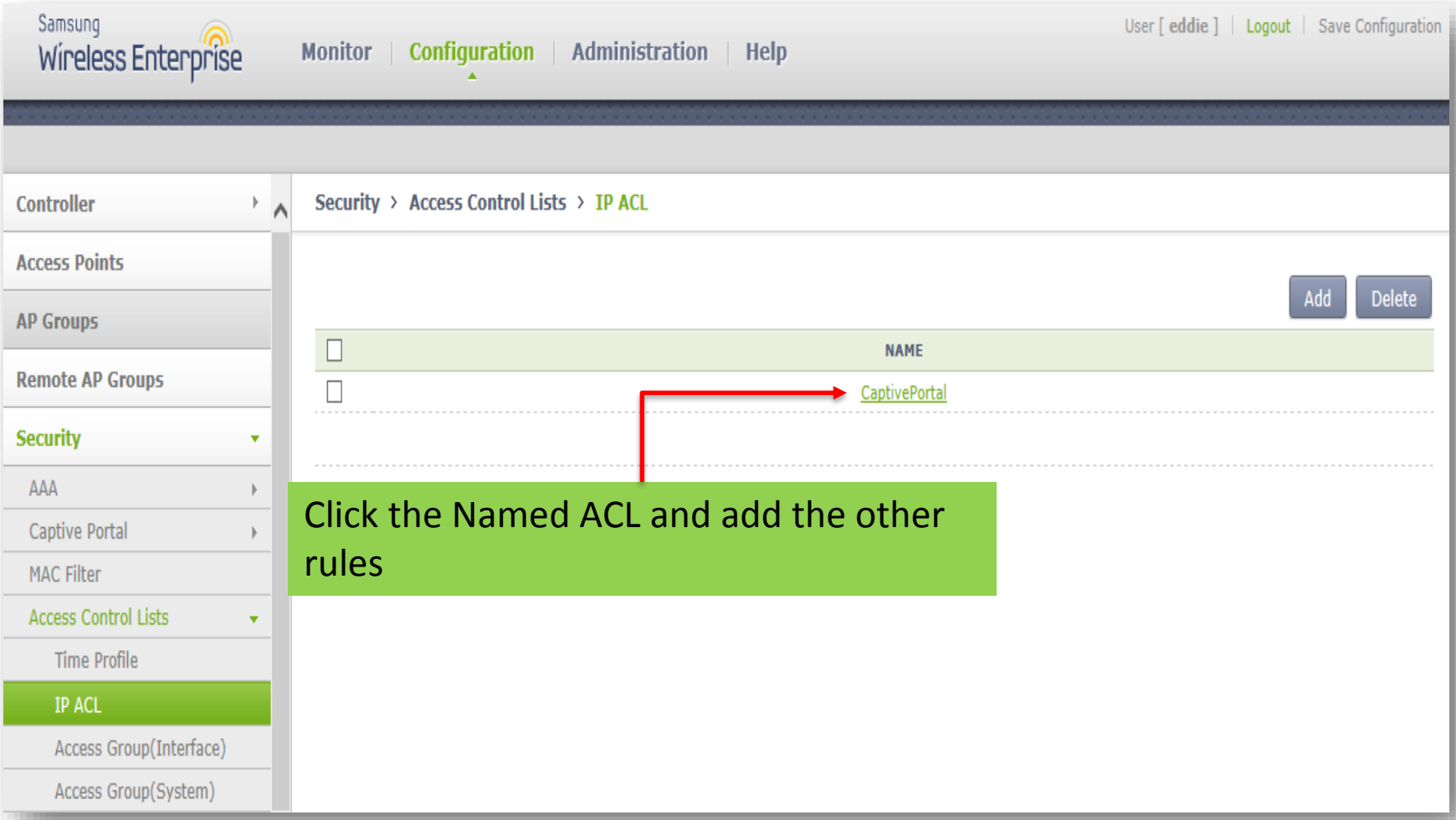


4.2.2 Access Control List

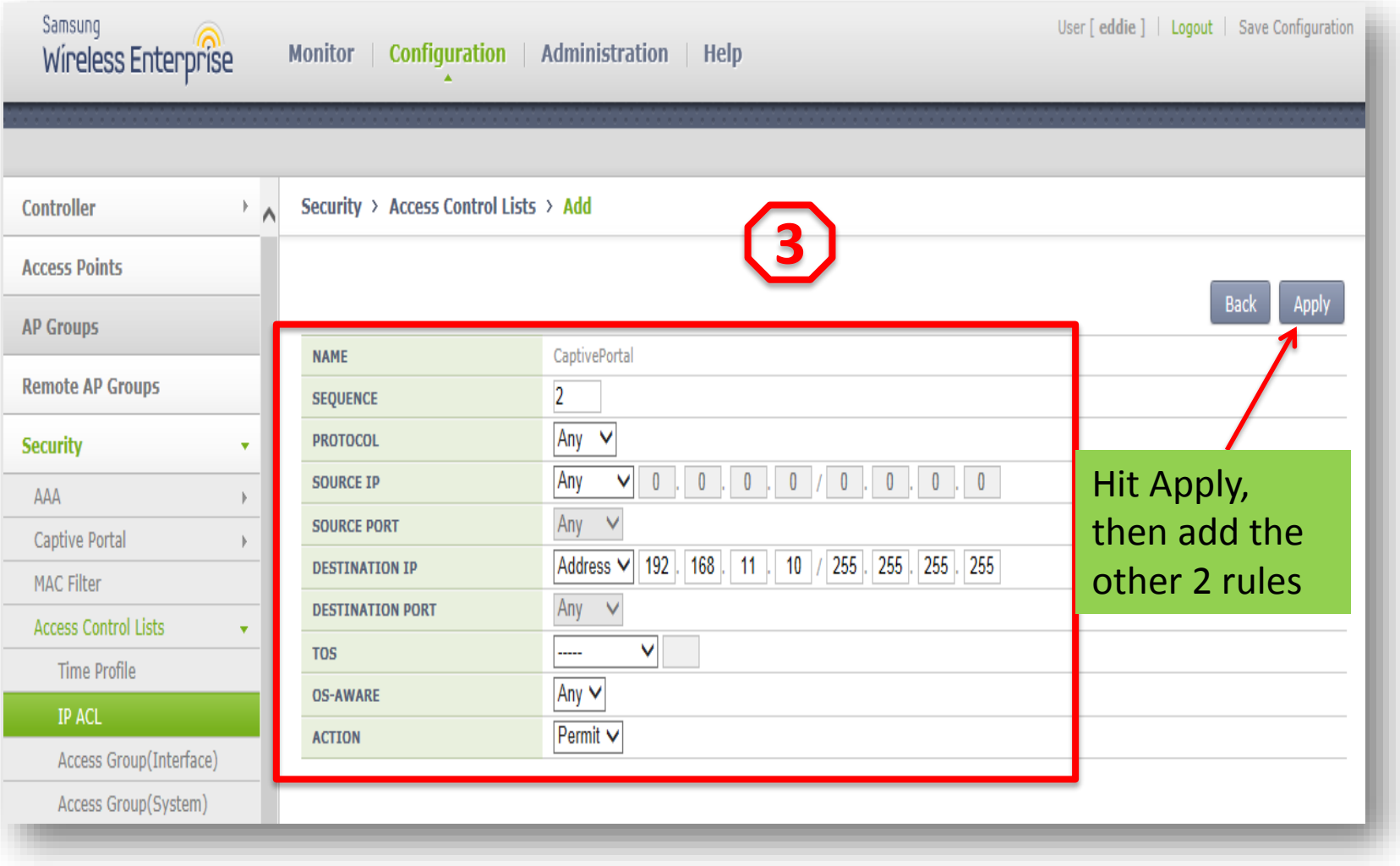
Here are the actions we need to create to setup our Captive Portal



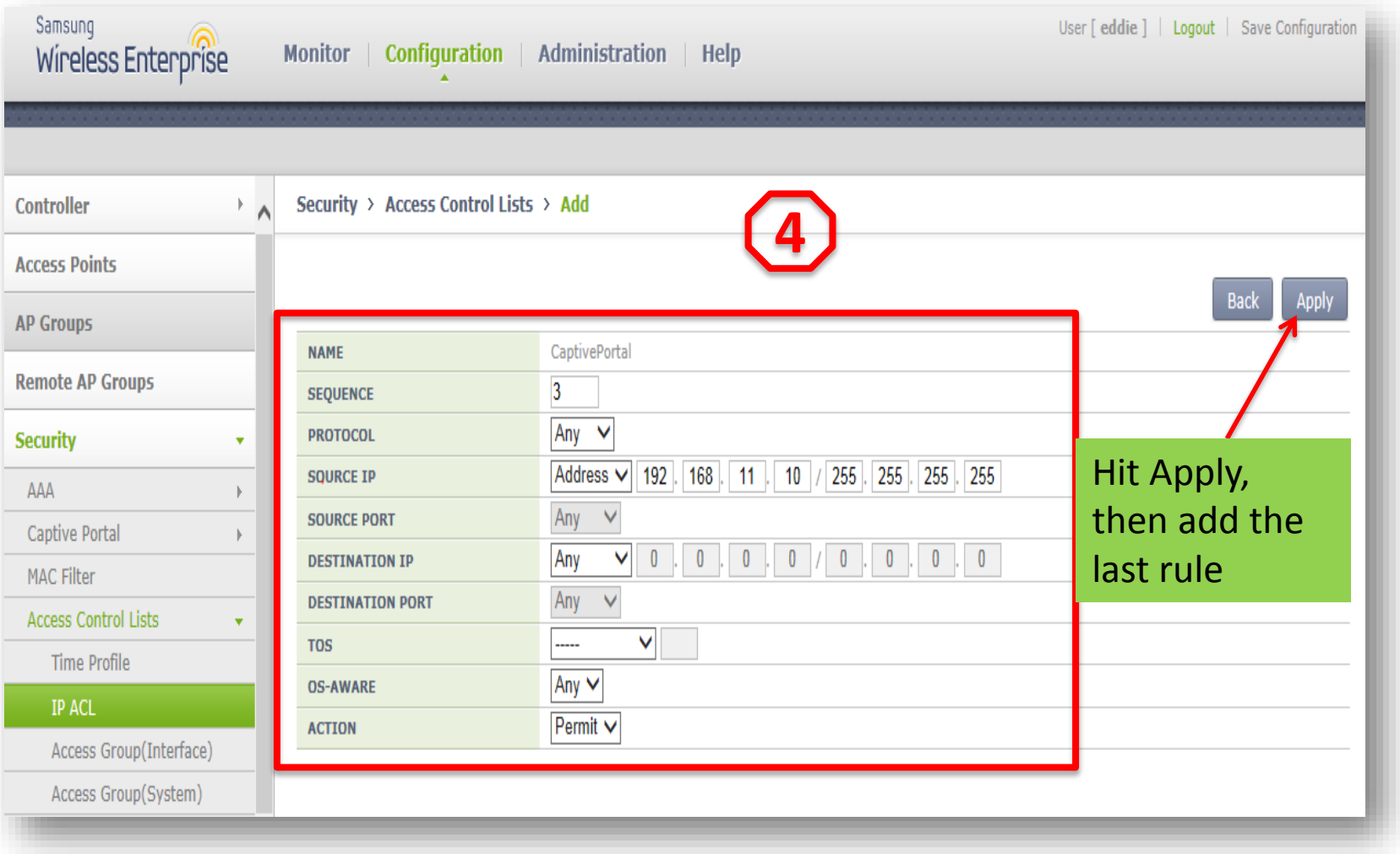
4.2.2 Access Control List



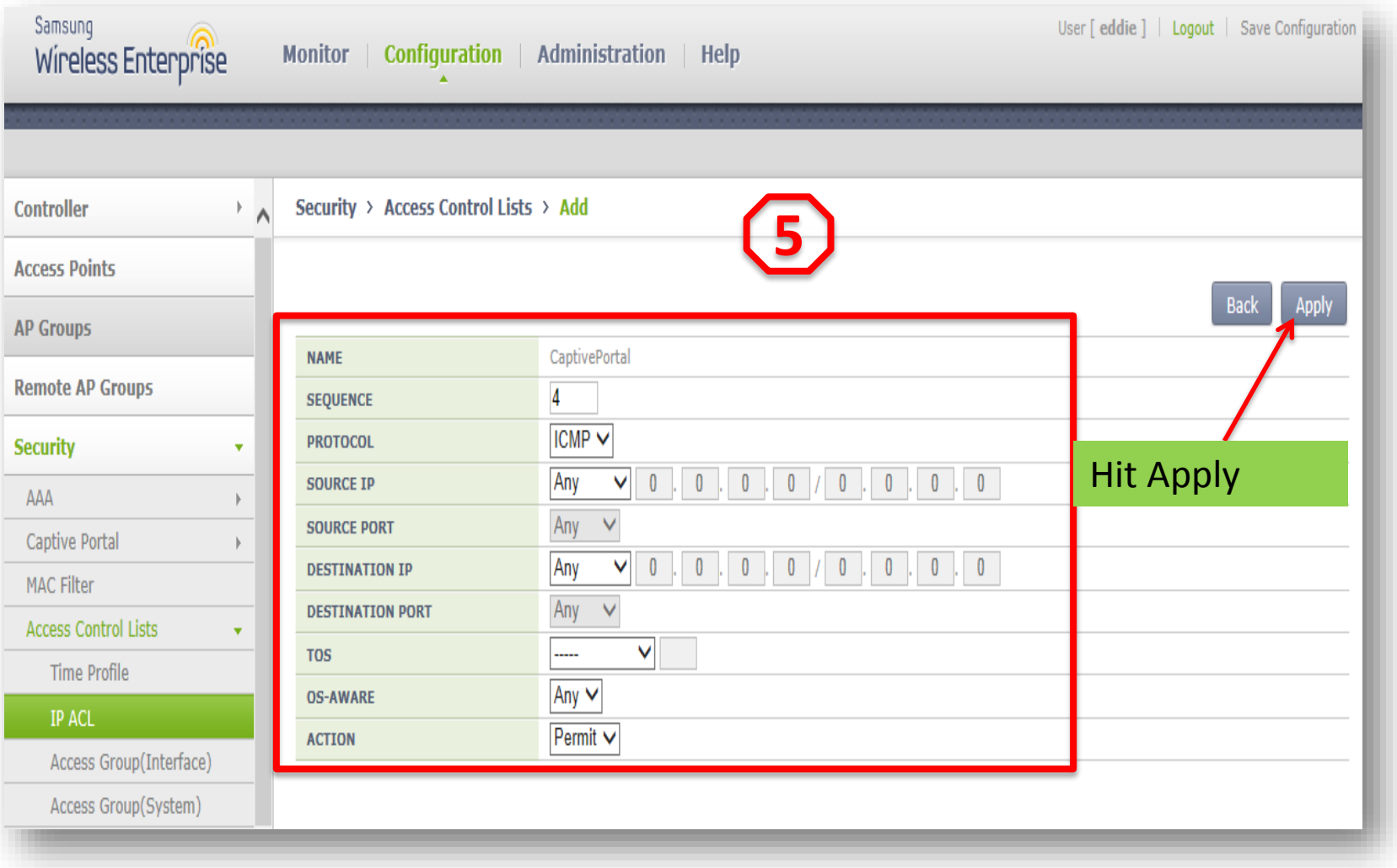
4.2.2 Access Control List



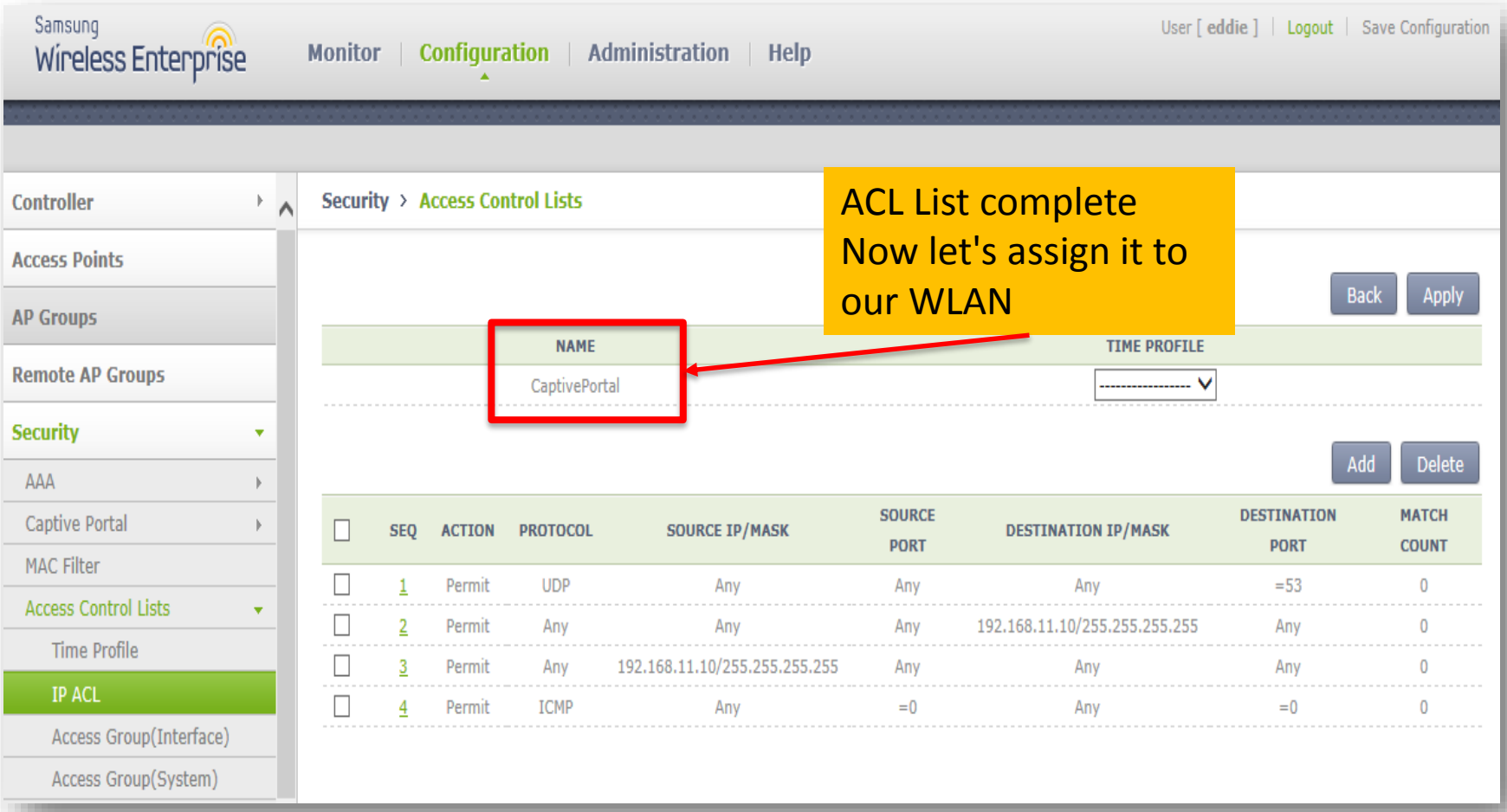
4.2.2 Access Control List



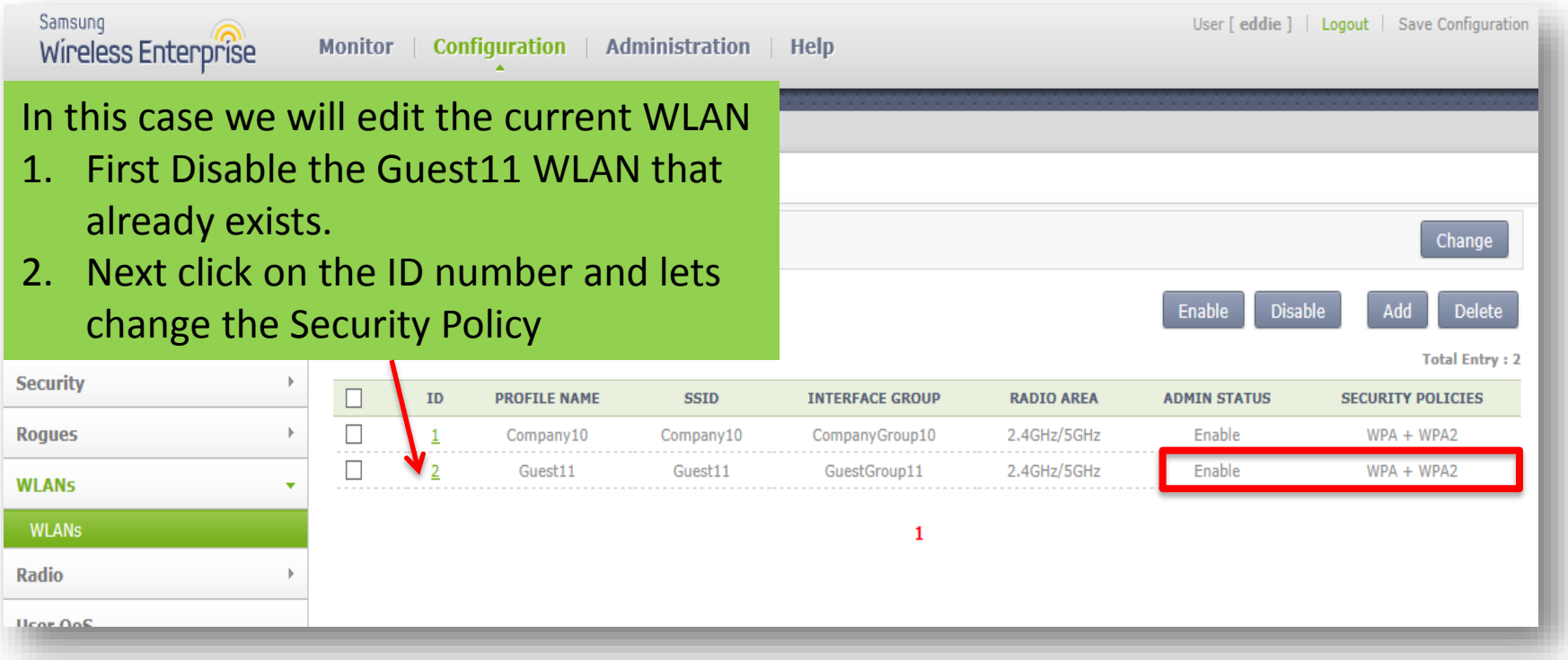
4.2.2 Access Control List



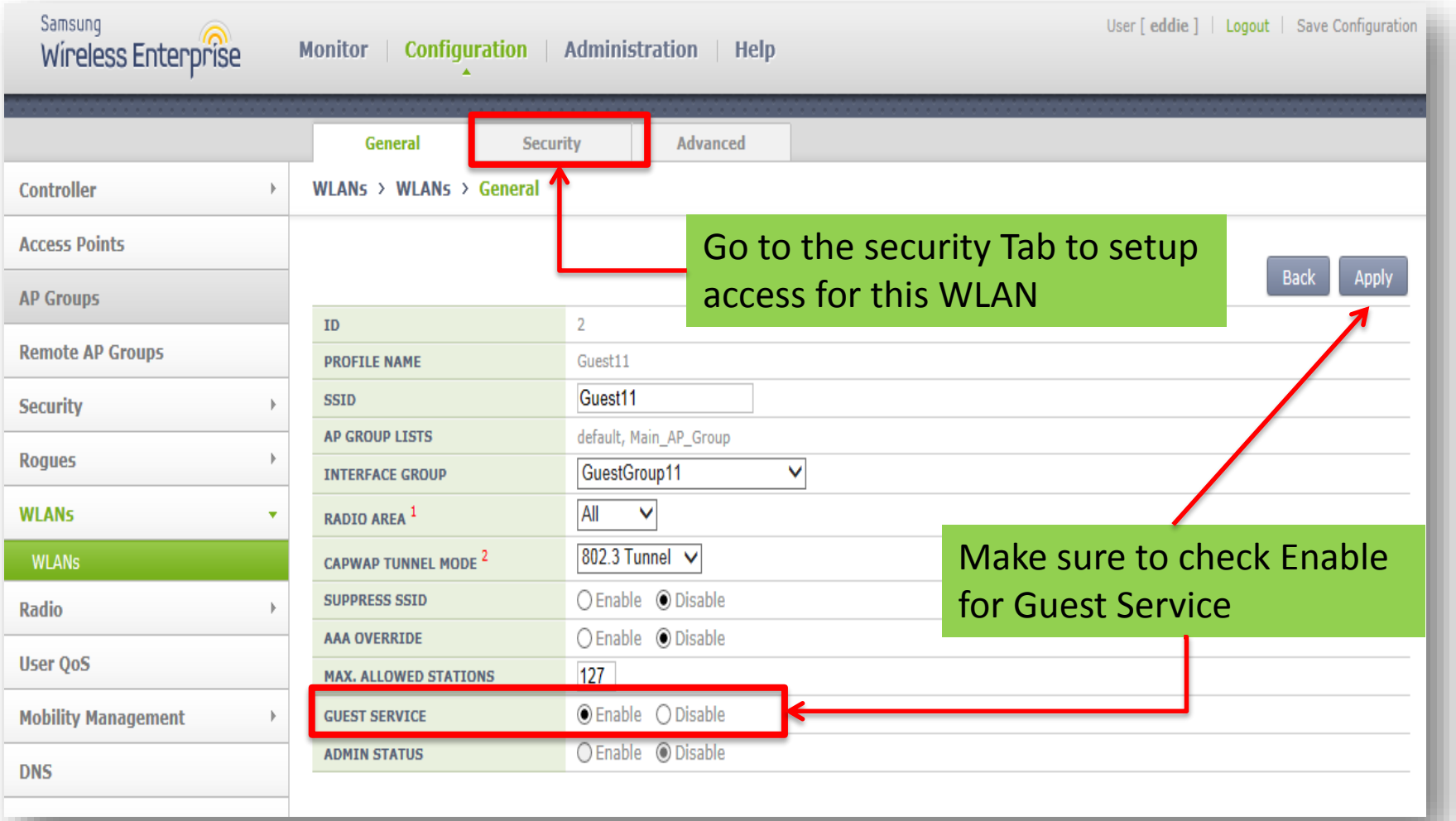
4.2.2 Access Control List



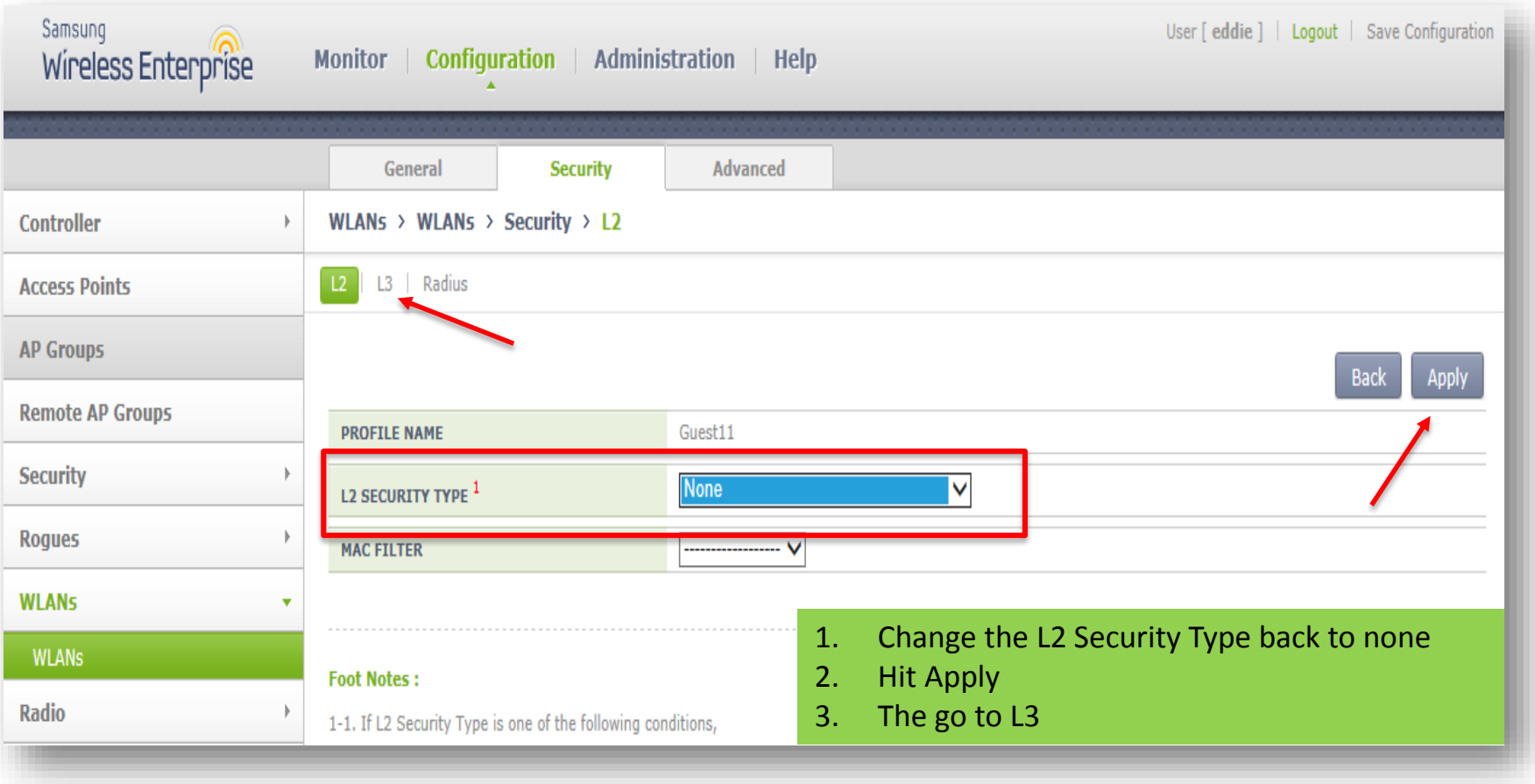
4.2.3 Guest Access WLAN



4.2.3 Guest Access WLAN

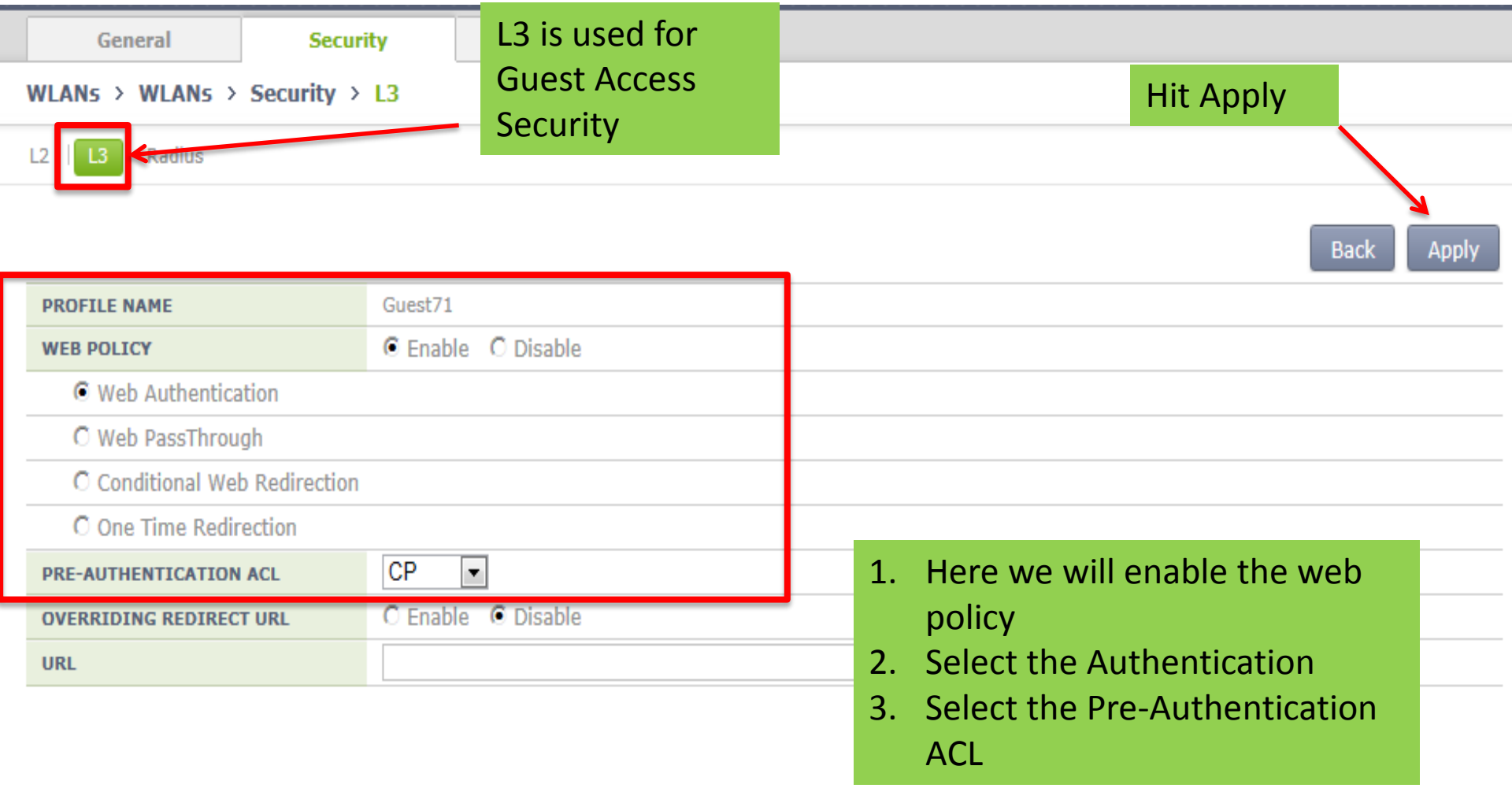


4.2.3 Guest Access WLAN



4.2.3 Guest Access WLAN

Samsung Wireless Enterprise™

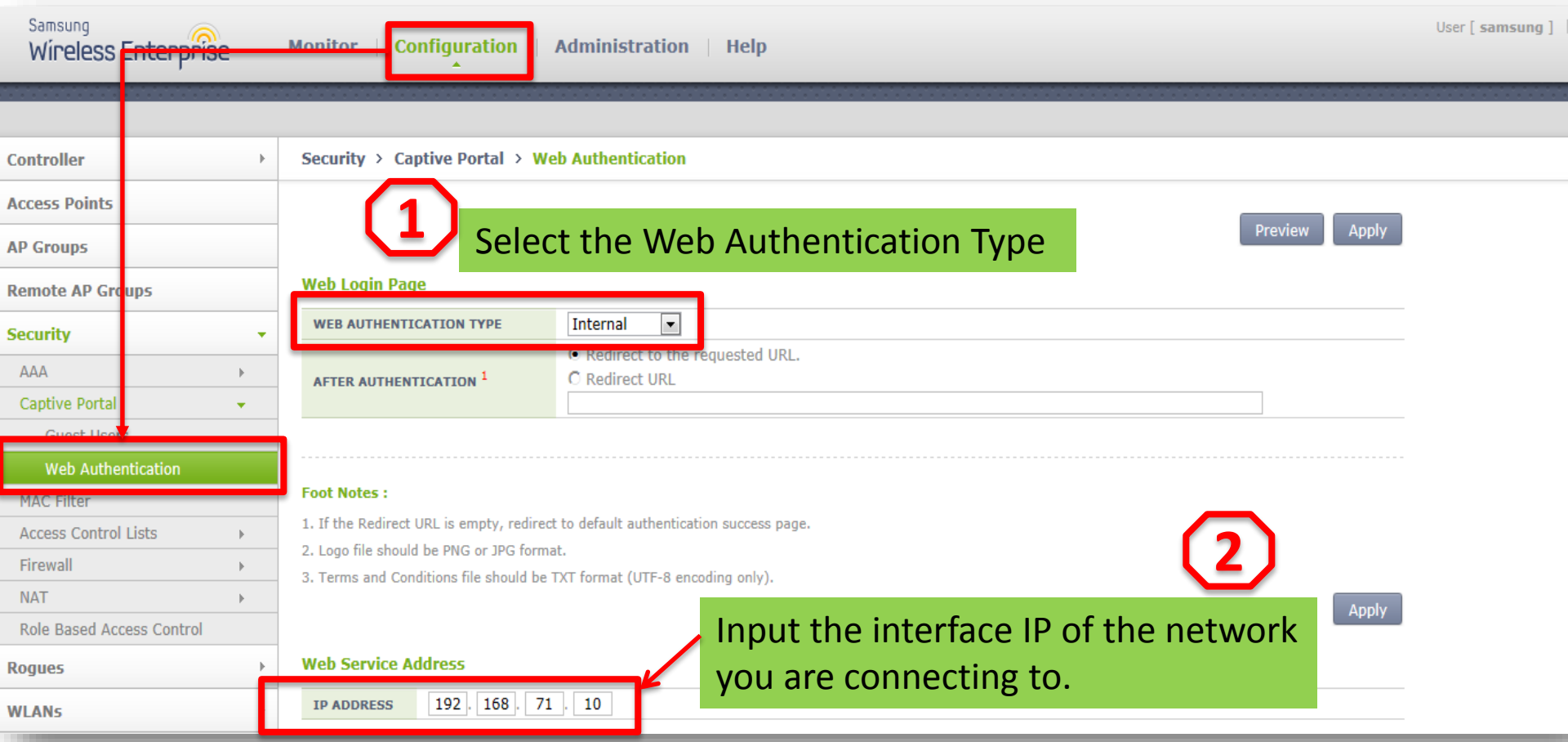


L3 is used for Guest Access Security

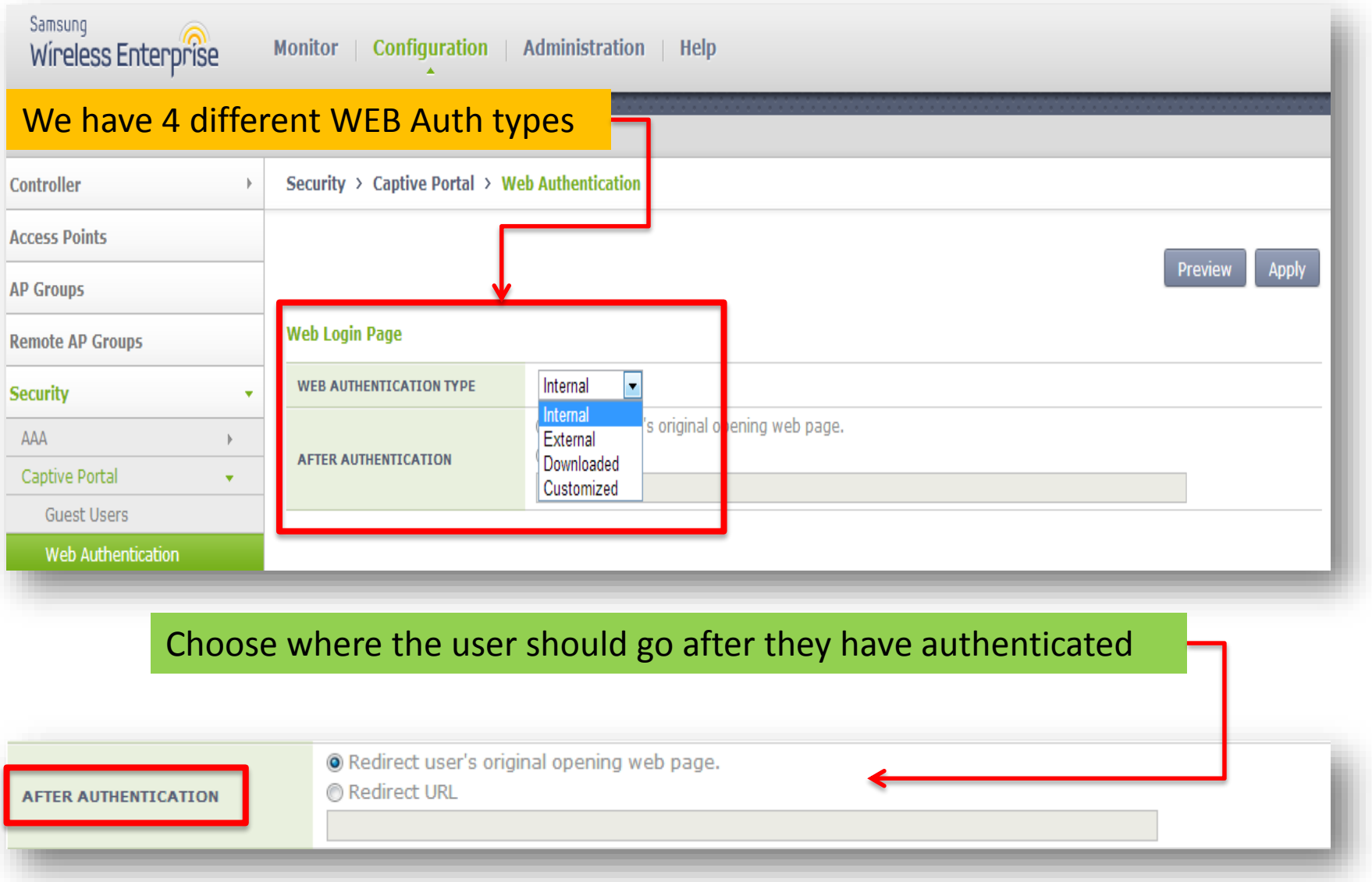
Hit Apply

1. Here we will enable the web policy
2. Select the Authentication
3. Select the Pre-Authentication ACL

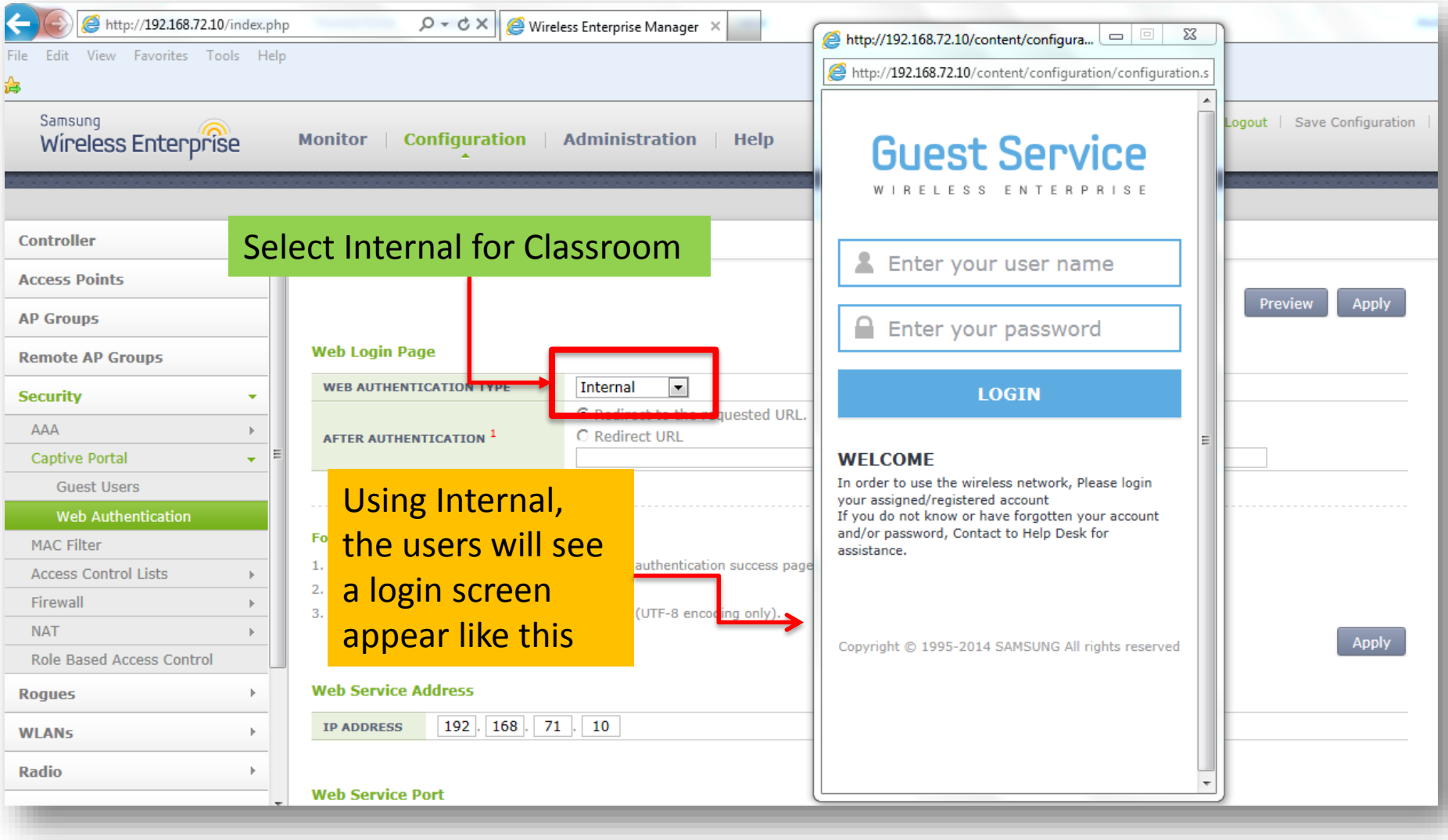
4.2.4 Web Authentication



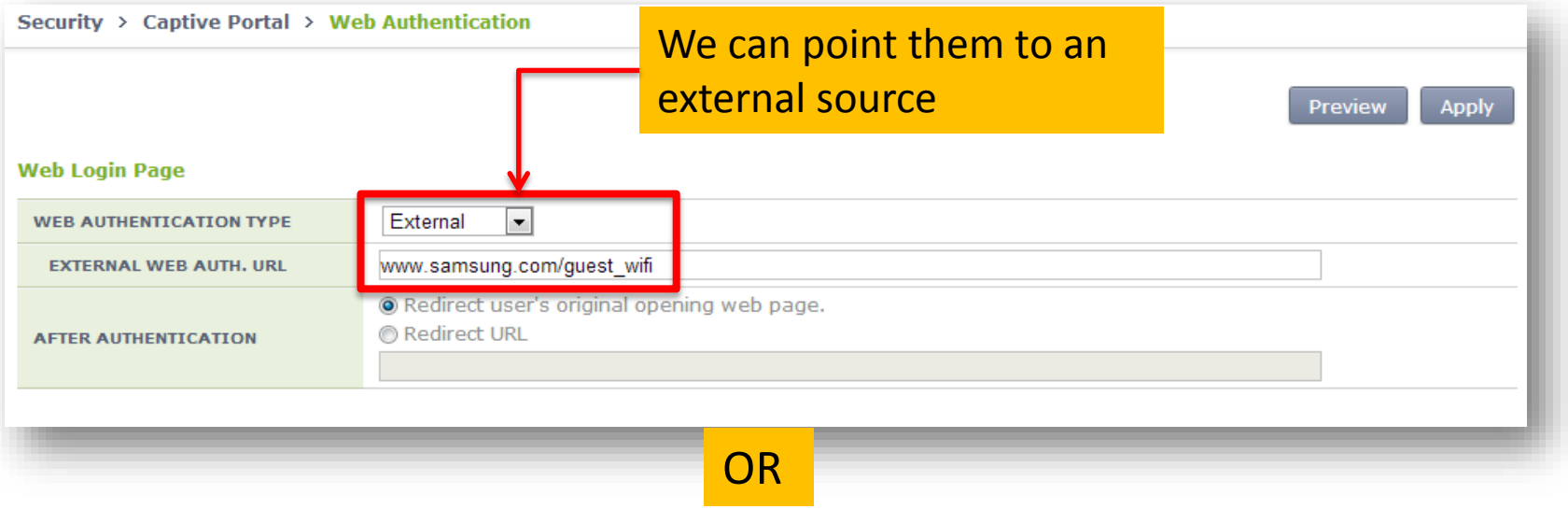
4.2.4 Web Authentication



4.2.4 Web Authentication

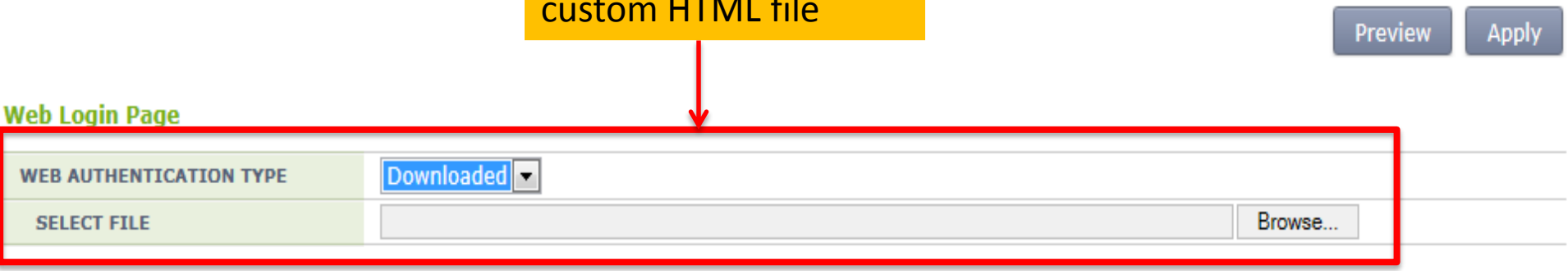


4.2.4 Web Authentication



OR

We can upload a custom HTML file



4.2.4 Web Authentication

Samsung Wireless Enterprise™

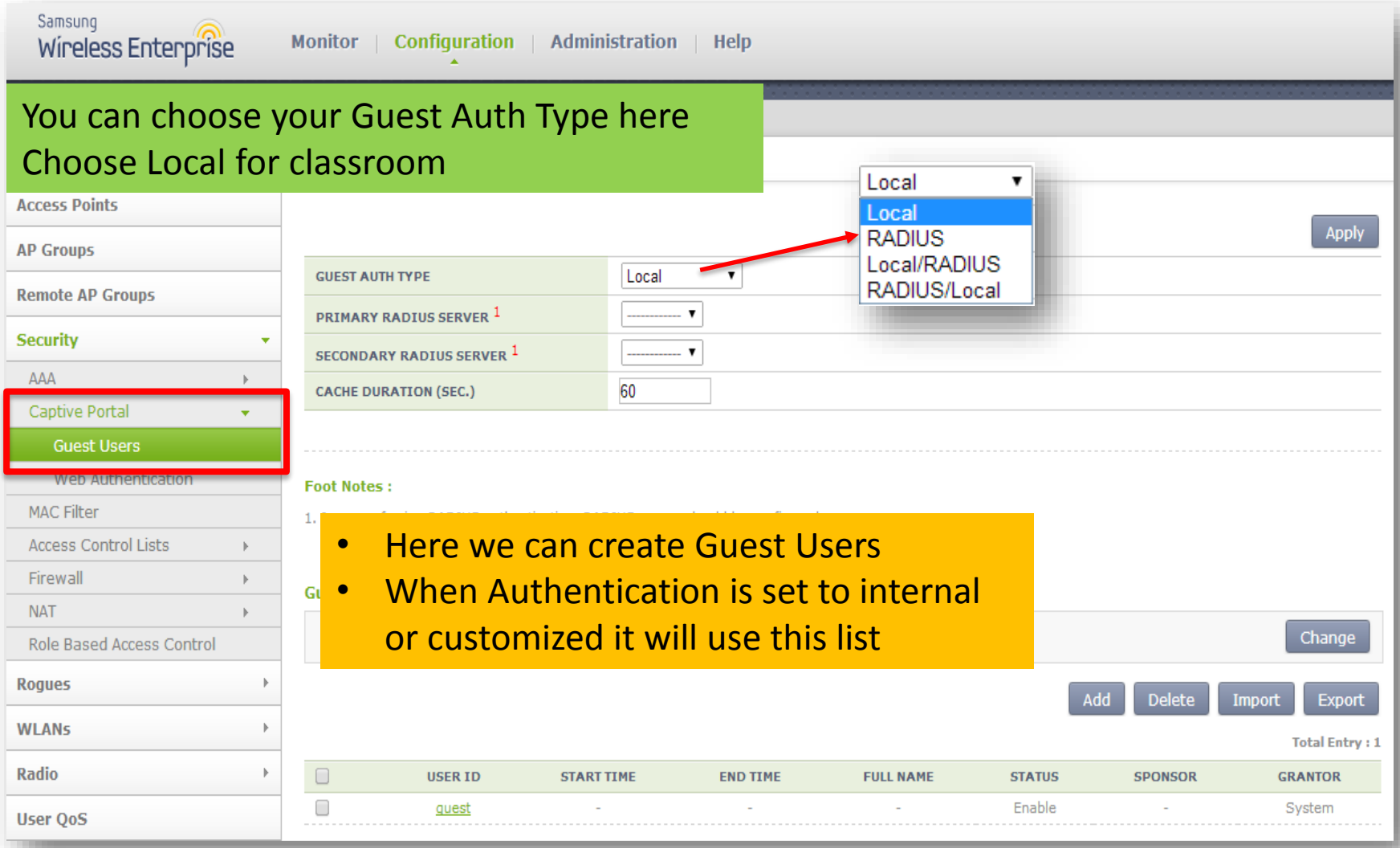
Using Customized we can editing the fields below

Preview Apply

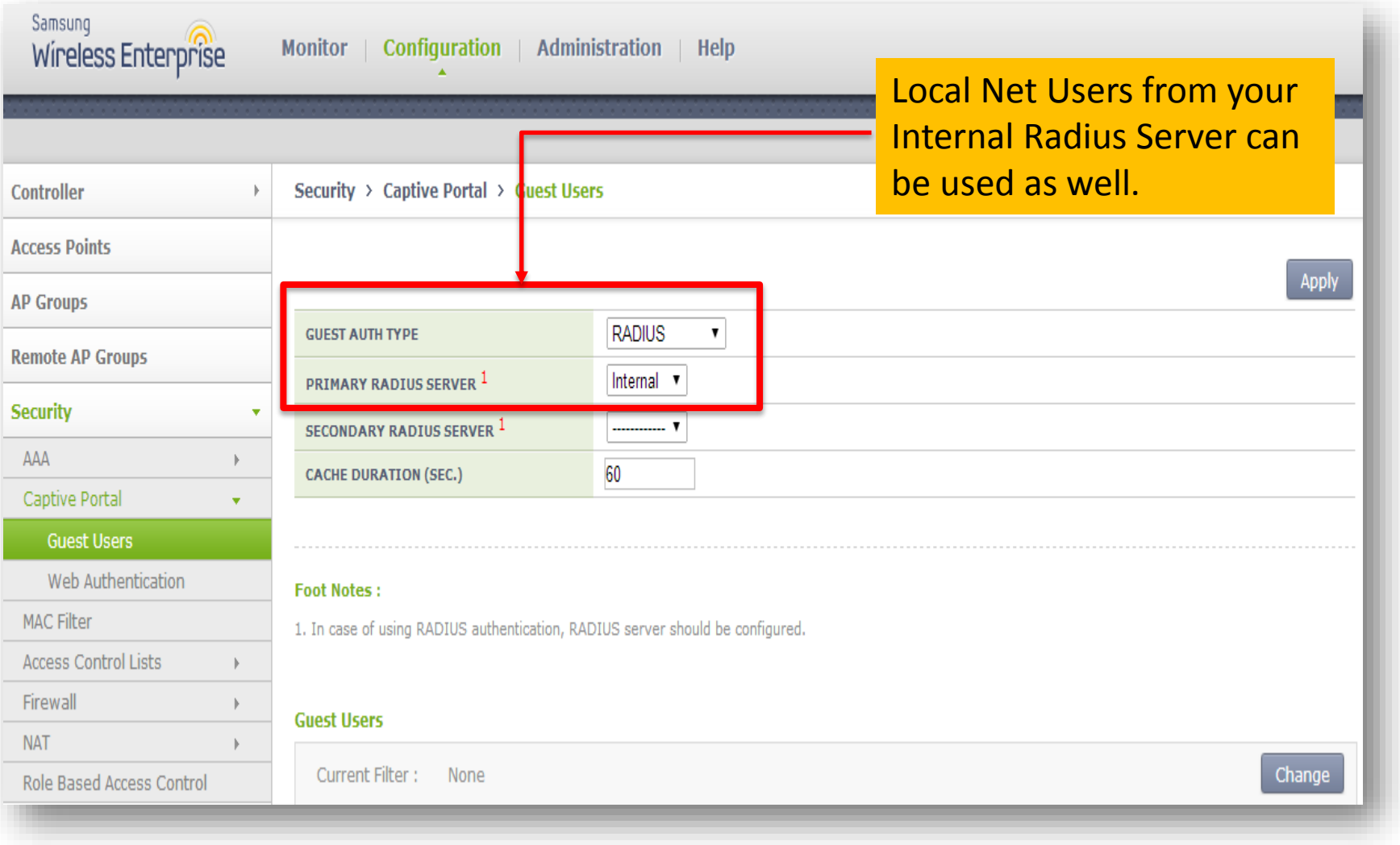
Web Login Page

WEB AUTHENTICATION TYPE	Customized
LOGO	Hide Show
SELECT FILE [2]	Browse...
HEADER	WELCOME
BODY	In order to use the wireless network, Please login your assigned/registered account. If you do not know or have forgotten your account and/or password, Contact to Help Desk for assi stance.
FOOTER	Copyright ** 1995-2014 SAMSUNG All rights reserved
TERMS AND CONDITIONS	Hide Show
SELECT FILE [3]	Browse...
COLOR	#0

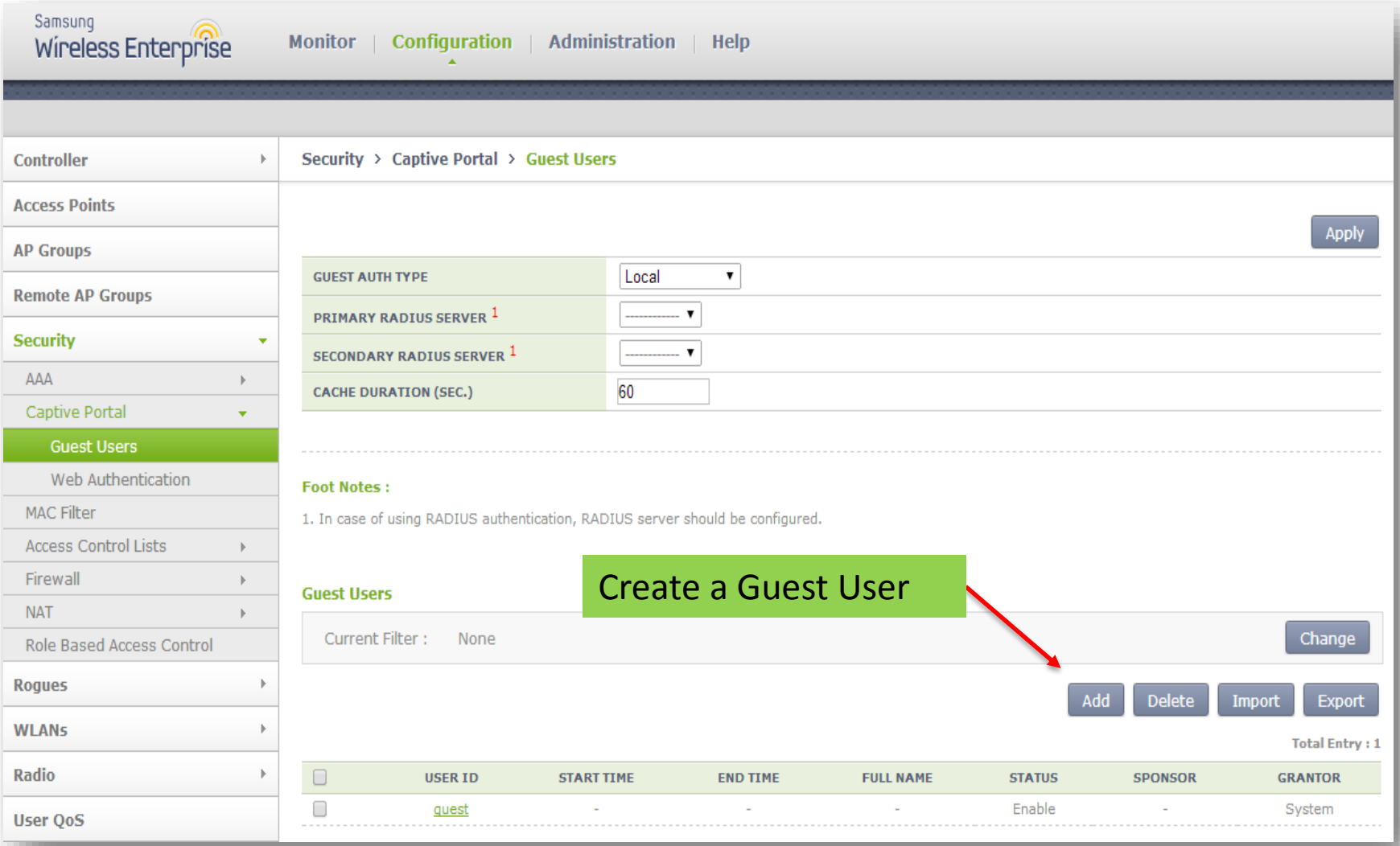
4.2.4 Creating Guest Users



4.2.4 Creating Guest Users

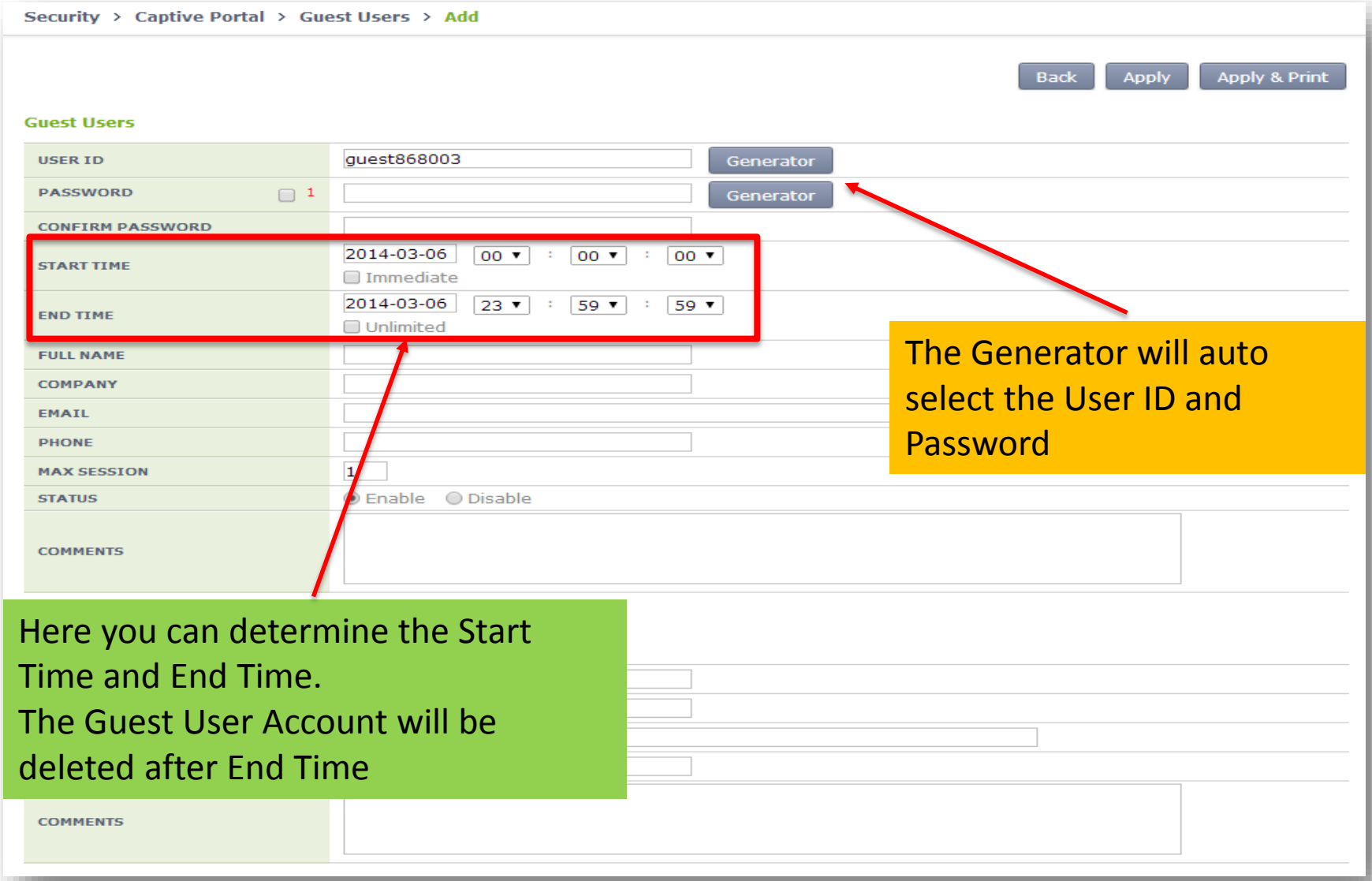


4.2.4 Creating Guest Users

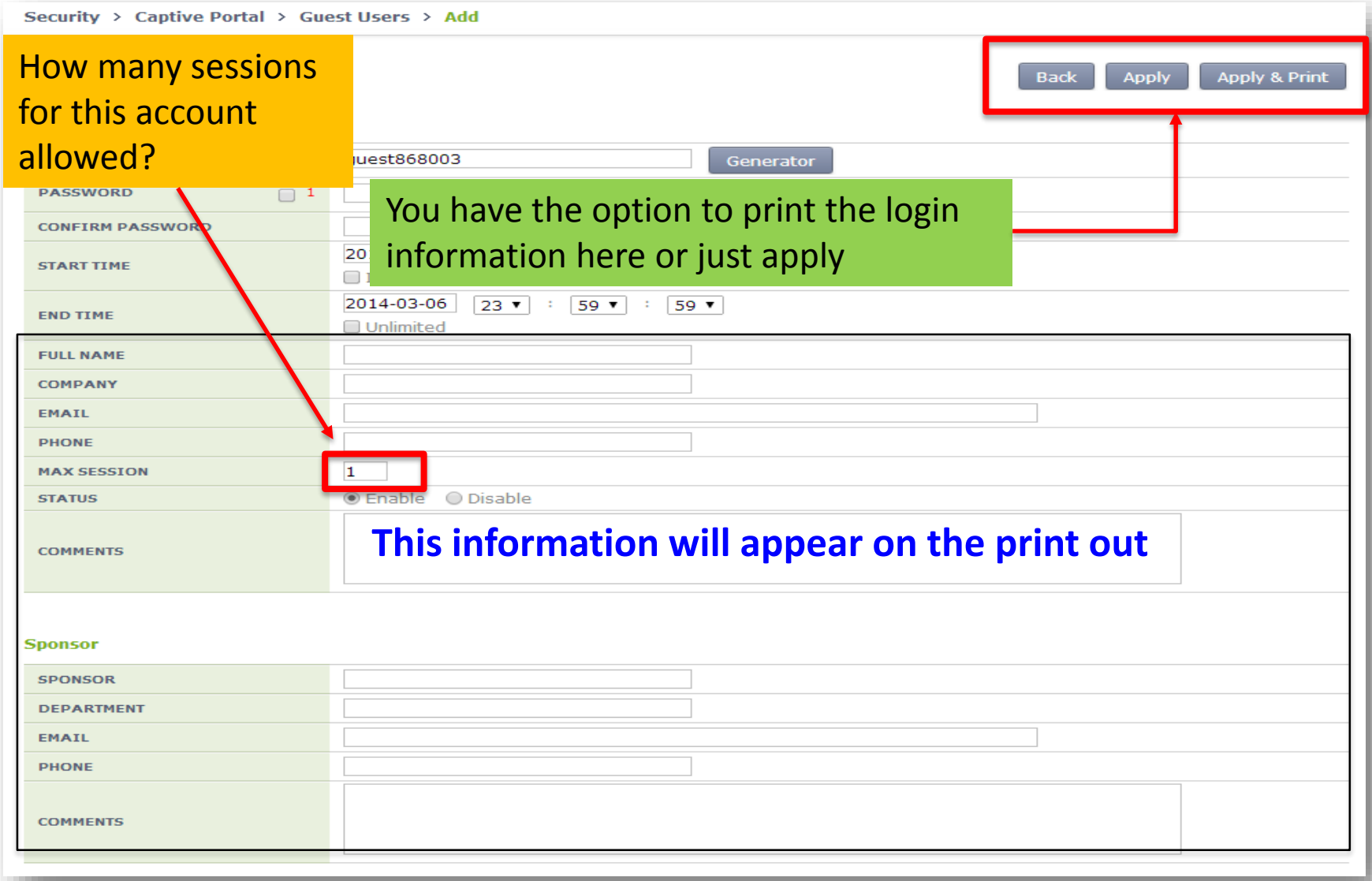


4.2.4 Creating Guest Users

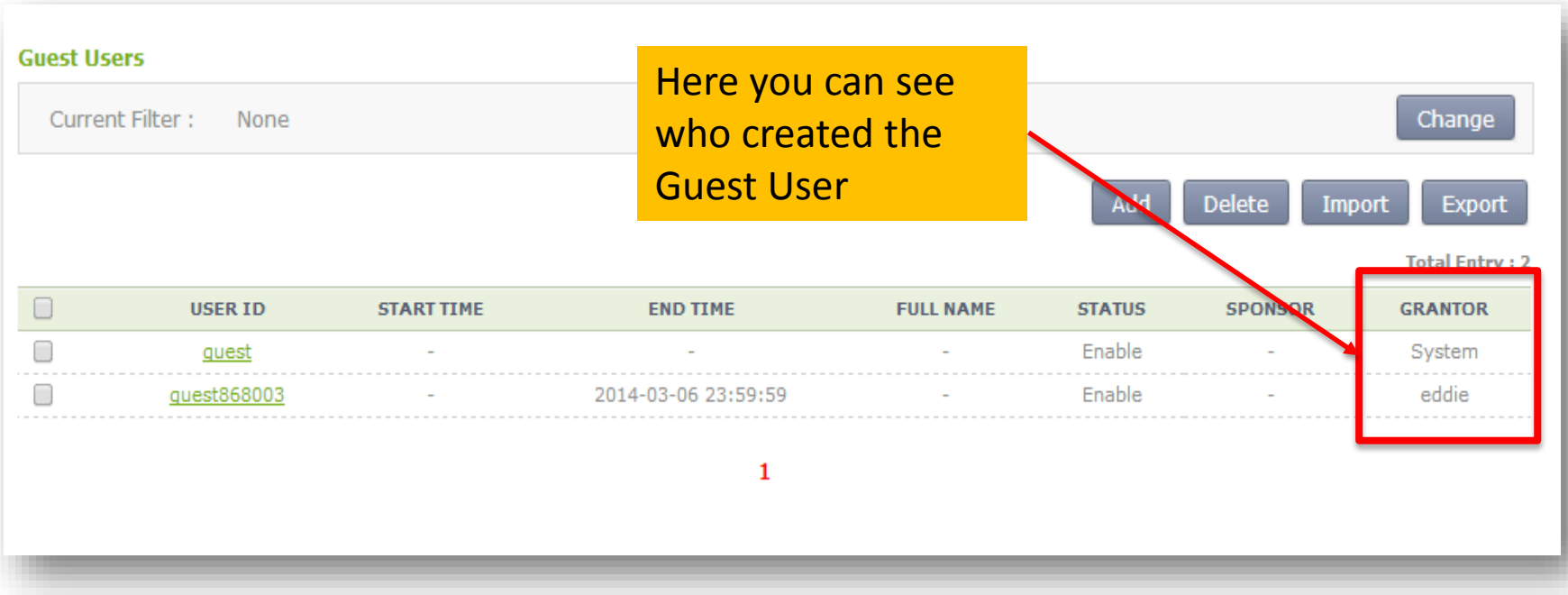
Samsung Wireless Enterprise™



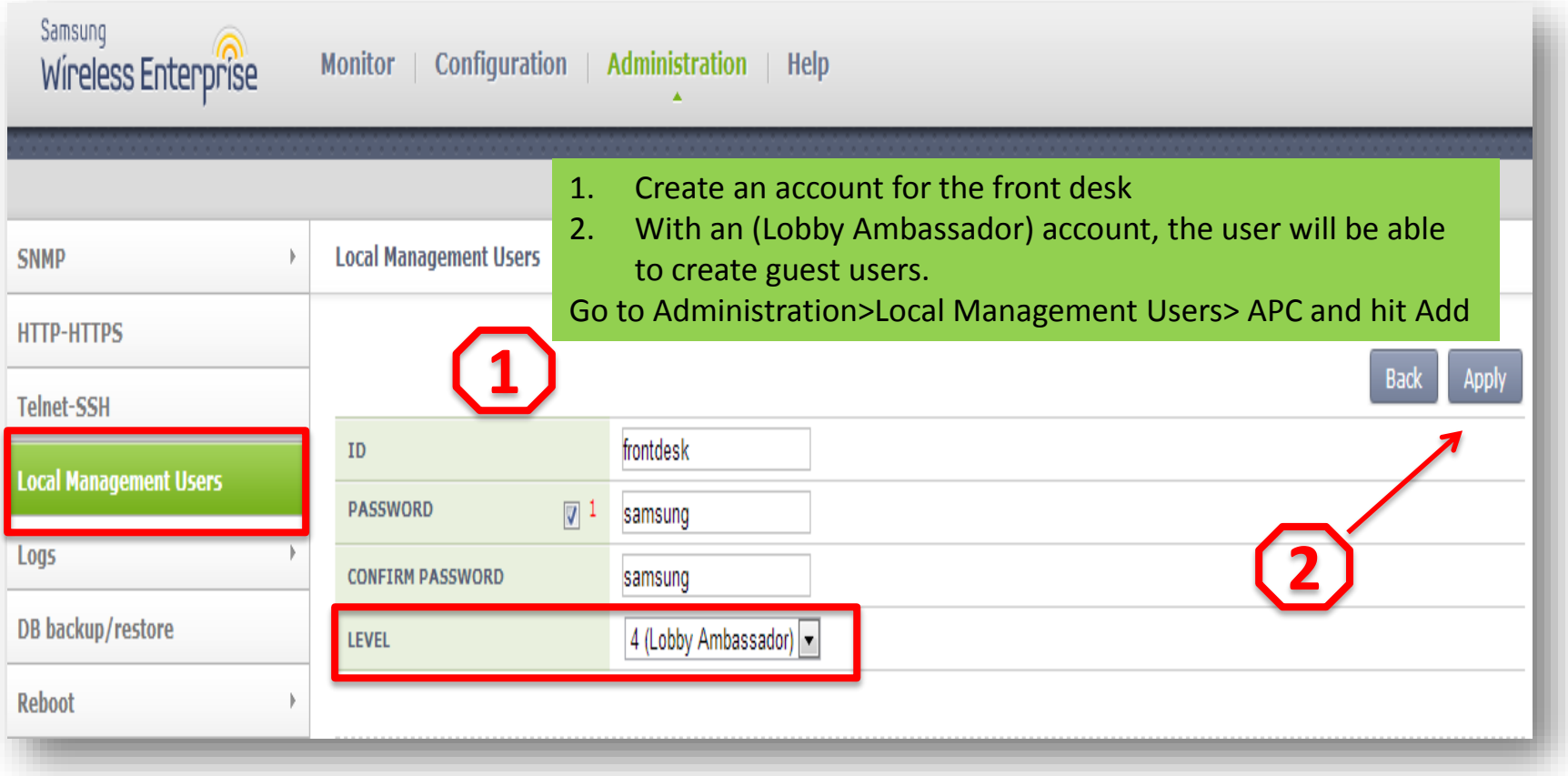
4.2.4 Creating Guest Users



4.2.4 Creating Guest Users



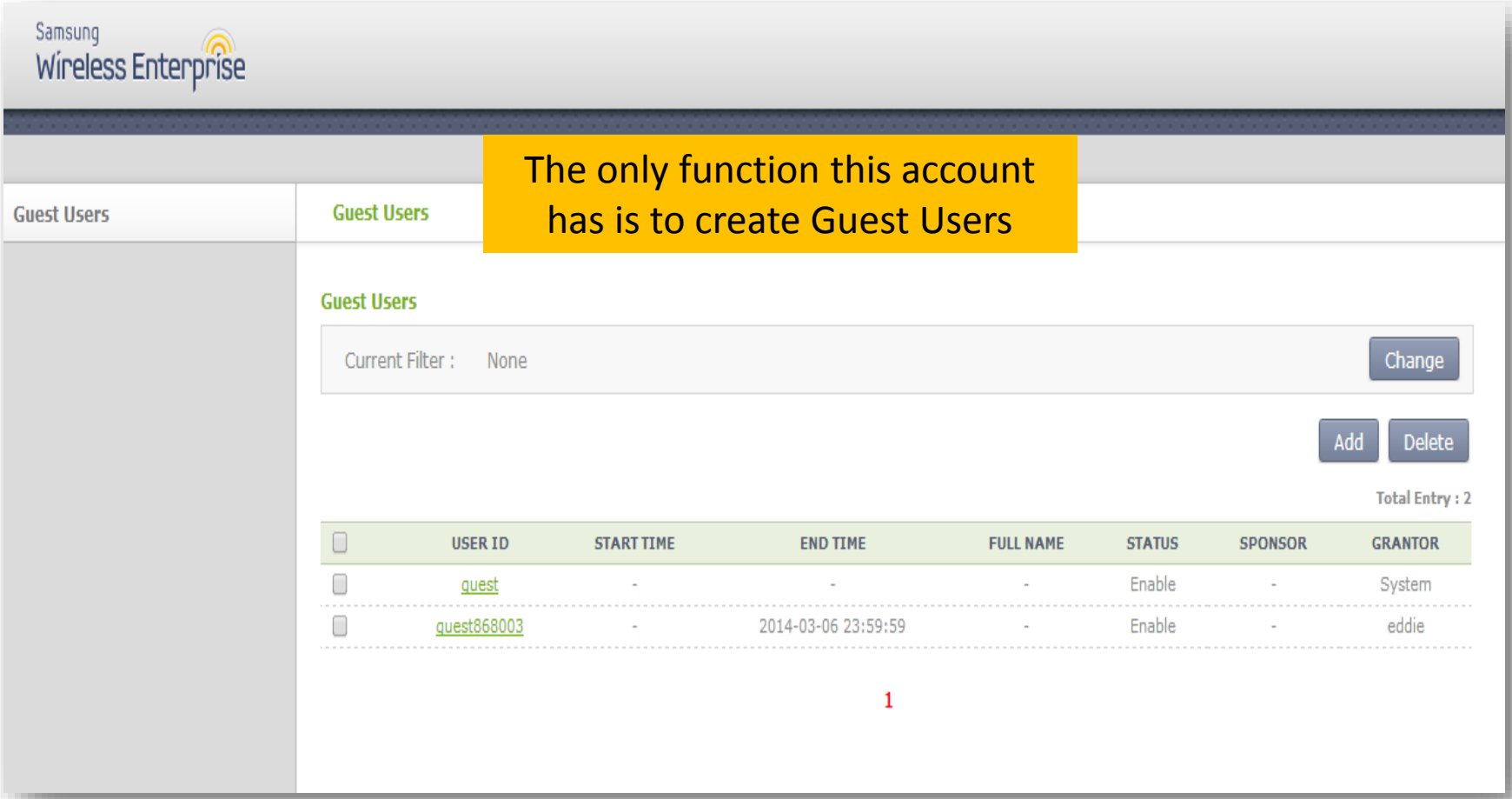
4.2.5 Lobby Ambassador



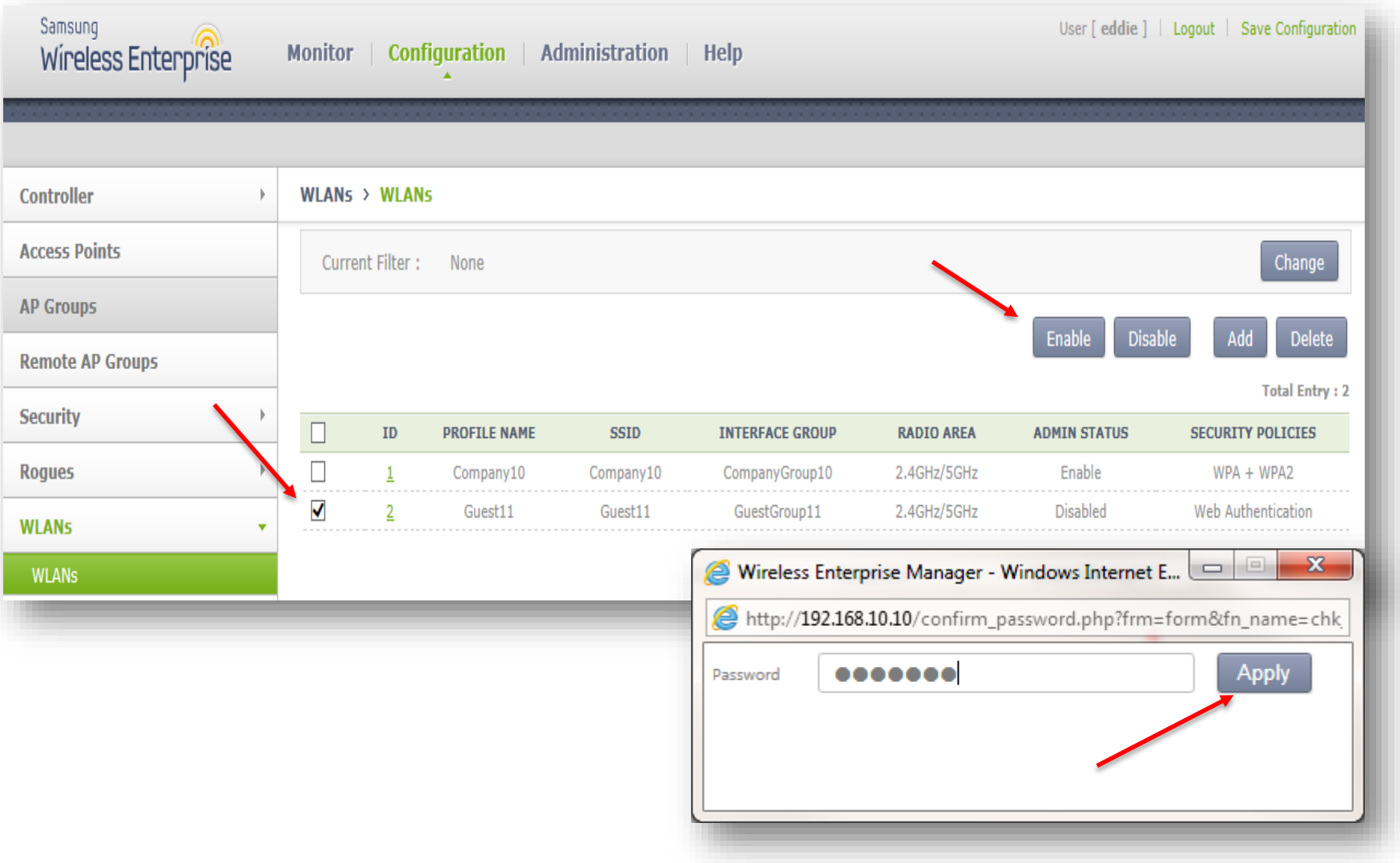
4.2.5 Lobby Ambassador

Samsung Wireless Enterprise™

4.2.5 Lobby Ambassador



4.2.6 Enable WLAN



Captive Portal “Lab 21”

Samsung Wireless Enterprise™

Lab 21 – (New WLAN Setup Example) (1/3)

Setup a WLAN that uses Captive Portal with Internal Web Authentication

First create the ACL for Captive Portal (1/4)

1. Go to Configuration → Security→ Access Control Lists → IP ACL → Add
   a. Name = CaptivePortal
   b. Sequence = 1
   c. Protocol = udp
   d. Source IP = Any
   e. Source Port = Any
   f. Destination IP = Any
   g. Destination Port = 53
   h. Action = Permit
   i. Apply

Captive Portal “Lab 21”

Samsung Wireless Enterprise™

Lab 21 – (New WLAN Setup Example) (1/3)

Setup a WLAN that uses Captive Portal with Internal Web Authentication

First create the ACL for Captive Portal (2/4)

1. Security→ Access Control Lists → IP ACL → CaptivePortal
    a. Sequence = 2
    b. Protocol = Any
    c. Source IP = Any
    d. Source Port = Any
    e. Destination IP = 192.168.xx.10/255.255.255.255
    f. Destination Port = Any
    g. Action = Permit
    h. Apply

Captive Portal “Lab 21”

Samsung Wireless Enterprise™

Lab 21 – (New WLAN Setup Example) (1/3)

Setup a WLAN that uses Captive Portal with Internal Web Authentication

First create the ACL for Captive Portal (3/4)

1. Security→ Access Control Lists → IP ACL → CaptivePortal
    a. Sequence = 3
    b. Protocol = Any
    c. Source IP = 192.168.xx.10/255.255.255.255
    d. Source Port = Any
    e. Destination IP = Any
    f. Destination Port = Any
    g. Action = Permit
    h. Apply

Captive Portal “Lab 21”

Samsung Wireless Enterprise™

Lab 21 – (New WLAN Setup Example) (1/3)

Setup a WLAN that uses Captive Portal with Internal Web Authentication

First create the ACL for Captive Portal (4/4)

1. Security→ Access Control Lists → IP ACL → CaptivePortal
    a. Sequence = 4
    b. Protocol = ICMP
    c. Action = Permit
    d. Apply

Lab 21 – (New WLAN Setup Example) (2/3)

Setup a WLAN that uses Captive Portal with Internal Web Authentication

1. Go to Configuration → WLANs → WLANs → Hit Change
   a. ID = 2
   b. Profile Name = GuestXX
   c. SSID = GuestXX
   d. Interface Group = GuestGroupXX
   e. Radio Area = All
   f. Guest Service = Enable
   g. Click on the ID #3 → Security → L3
   h. WEB Policy = Enable with Web Authentication
   i. Pre-Authentication ACL = CaptivePortal → Apply
   j. Enable the WLAN
2. Go to Configuration → Security → Captive Portal → Web Auth
   a. Web Auth Type = Internal
   b. After Auth = optional setup
   c. Input the Web service address
   d. Hit Apply

Captive Portal “Lab 21”

Samsung Wireless Enterprise™

Lab 21 – (New WLAN Setup Example) (3/3)

Setup a WLAN that uses Captive Portal with Internal Web Authentication

1. Go to Configuration → Security → Captive Portal → Guest Users
   a. Guest Auth Type = Local
   b. Click Add = Create a user ID to be able use this service

2. Test
   a. Connect your PC or Phone to the SSID and login using the created guest ID

Samsung Wireless Enterprise™

4.3 Web Passthrough

- 4.3.1 Introduction
- 4.3.2 ACL Rules
- 4.3.3 Setup Web Passthrough

4.3.1 Introduction

Samsung Wireless Enterprise™

Introduction

- When the wireless users try to access Internet at the first time, Users are redirected to the web page specified by Web Passthrough.
- Web Passthrough is a useful feature that is used for guest access.
- The process of web passthrough is similar to that of web authentication except that authentication credentials are required for web authentication.

Process of Web Passthrough

- User associate a WLAN with no security and get DHCP IP address.
- When user open a web browser, user sends a specific HTTP get message and APC returns HTTP Redirect message to the user.
- User's web page is redirected to the redirected web page.

Limitations

- If WLAN is configured as local bridging mode, Web Passthrough does not work (PKG ver. 1.4.12)

4.3.2 ACL Rules

Samsung Wireless Enterprise™

Applying ACL to WLAN

- Web passthrough is applied to the WLAN with no security.
- ACL is applied to prevent users from accessing unauthorized destinations but a part of packets from/to user must be allowed to establish a basic communication.

ACL Rules for Web Passthrough

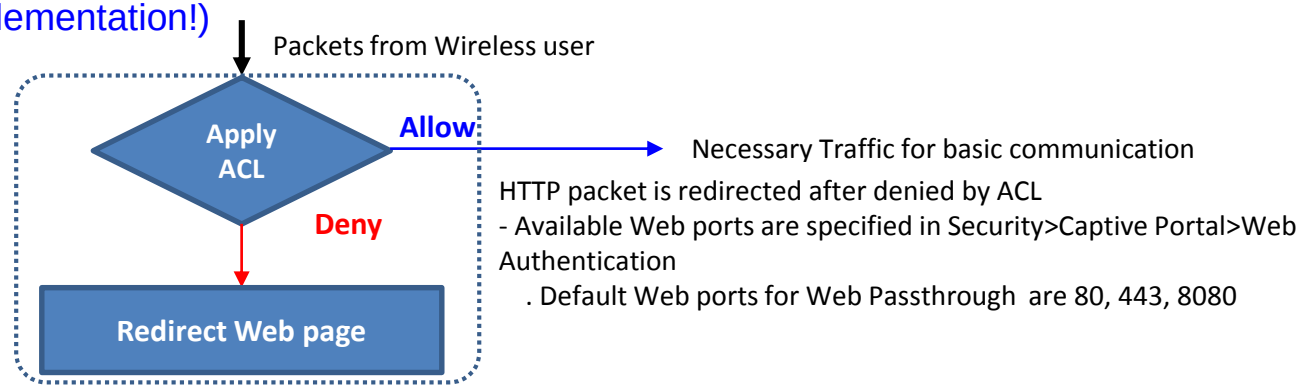
- **Allowed Rules**
  - *DNS flow*
  - *DHCP flow*
  - *Redirected Web server defined by administrator*
  - *(Optional) HTTP Proxy Server's IP Address*
  - *(Optional) The IP address of Server to download some applications*

  → *All the above flows are from/to wireless users*
- **Denied Rules**

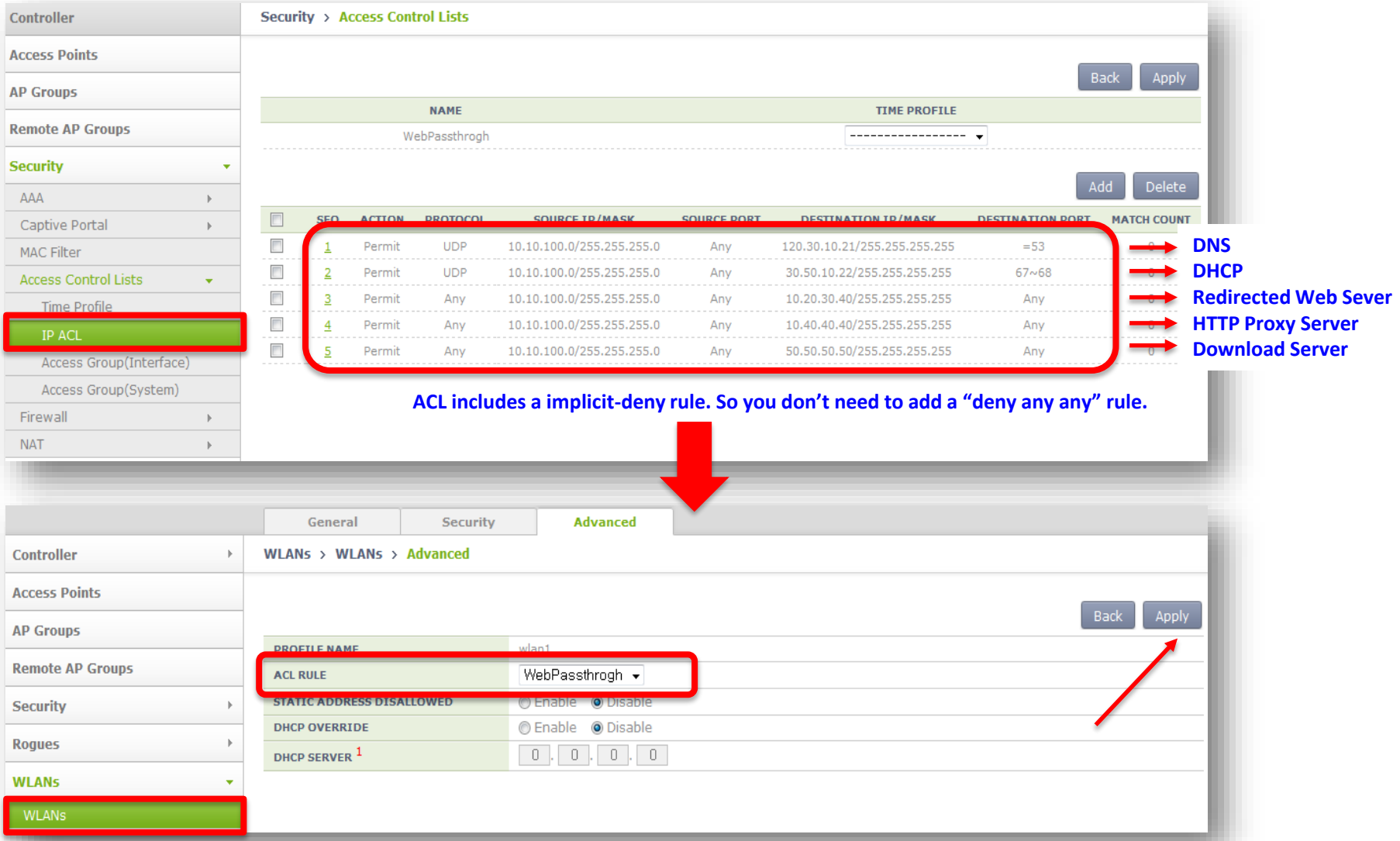
Traffic Flows that Administrator does not intend to allow on the WLAN

APC makes a redirection for HTTP get message only when the packet is matched by ACL denied rule.

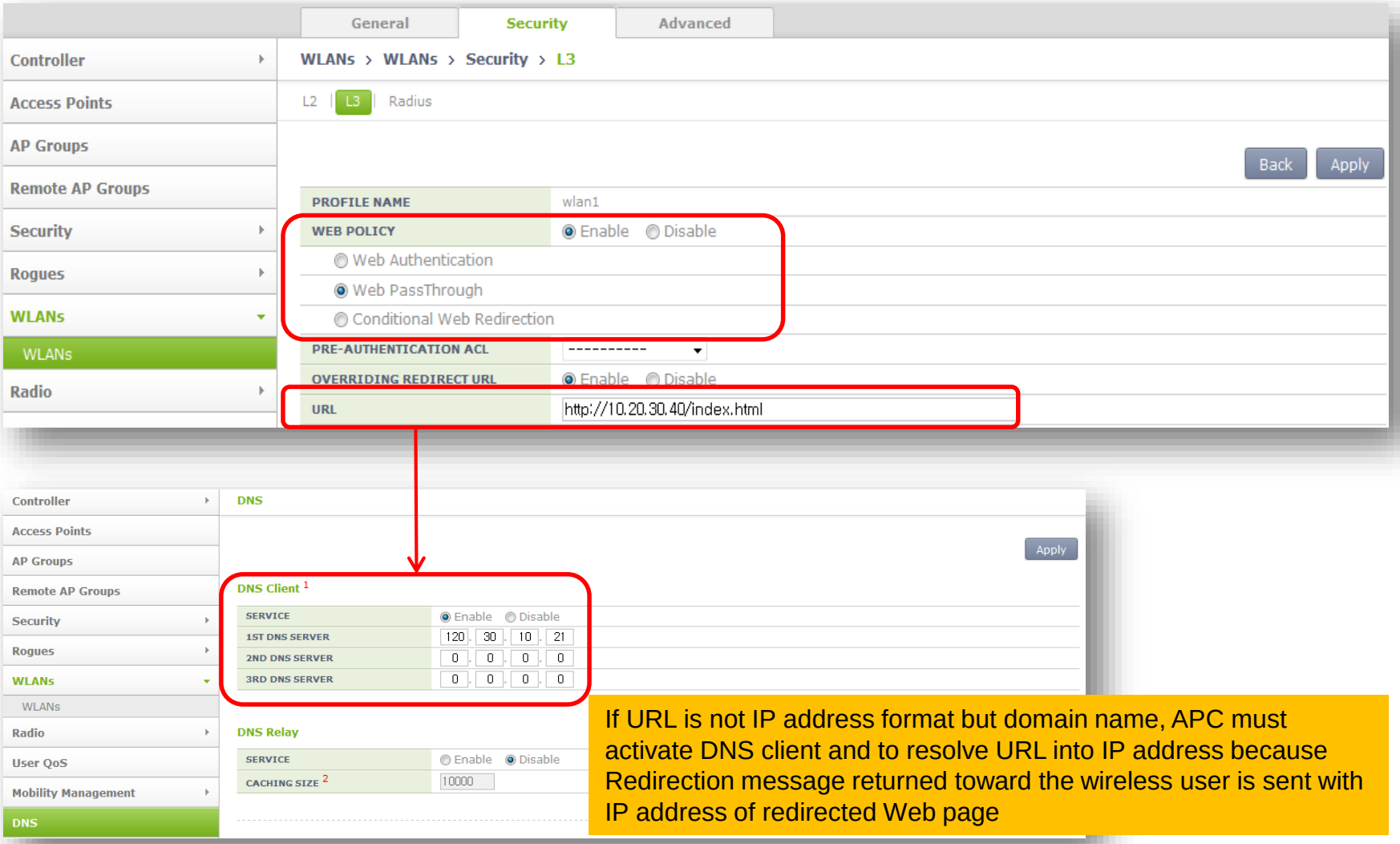
(Internal implementation!)



4.3.3 Setup Web Passthrough



4.3.3 Setup Web Passthrough



If URL is not IP address format but domain name, APC must activate DNS client and to resolve URL into IP address because Redirection message returned toward the wireless user is sent with IP address of redirected Web page

Samsung Wireless Enterprise™

4.4 Conditional Web Redirection

- 4.4.1 Introduction
- 4.4.2 ACL Rules
- 4.4.3 Setup Conditional Web Redirect

4.4.1 Introduction

Samsung Wireless Enterprise™

Introduction

- With Conditional Web Redirection, User is redirected to a particular web page when user reaches the expiration date or when the user needs to pay a bill for continued wireless service.
- When user's authentication period is expired and user try to authenticate, Radius server returns Samsung-Url-Redirect information and APC redirects to user's specified URL when they open a browser.

Process of Conditional Web Redirection

1. Radius server detects that user reaches the expiration date or needs to pay a bill for wireless service.
2. When user (re)authenticates after Step2, Radius server returns {Samsung-Url-Redirect} or {Samsung-Url-Redirect, Samsung-Url-Redirect-Acl} message.
3. When user open a browser, user is redirected to Redirected web page. Conditional Web Redirection is similar to the Web Passthrough but ACL rule for Conditional Web redirection is provided by Samsung-Url-Redirect-Acl message from Radius server or Pre-auth-ACL on WLAN L3 security can be applied.

Preconditions

- To use Conditional Web Redirection, Radius server must have Samsung dictionaries related to Conditional Web redirection

Limitations

- If WLAN is configured as local bridging mode, Conditional Web Redirection does not work (PKG ver. 1.4.12)
- Pre-auth-ACL feature on the WLAN does not work at PKG version 1.4.x (Available after 1.5.0)

4.4.2 ACL Rules

Applying ACL to WLAN

- Conditional Web Redirection can be applied to the WLAN with 802.1x.
- ACL is applied to prevent users from accessing unauthorized destinations but a part of packets must be allowed to establish a basic communication. This ACL has been used only until authentication is successful

ACL Rules for Conditional Web Redirection

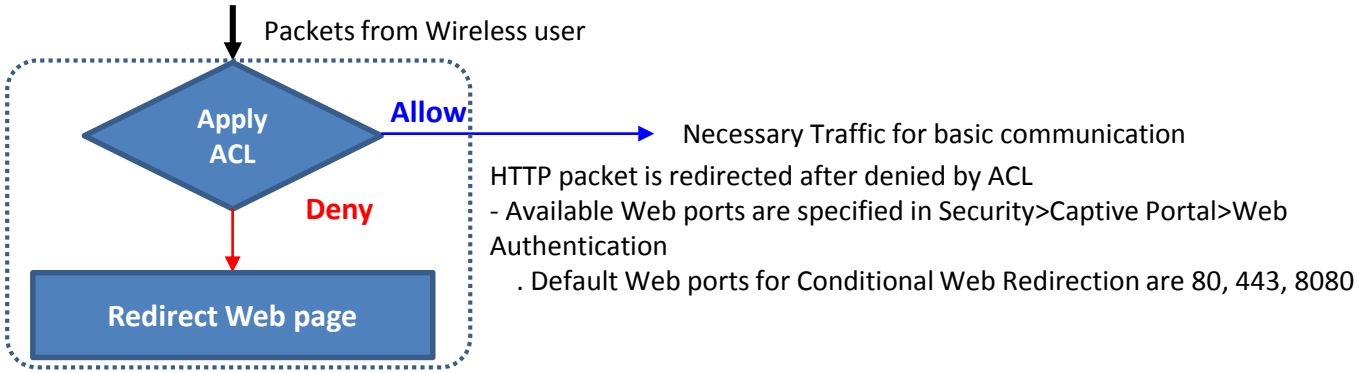
- **Allowed Rules**
  - *DNS flow*
  - *DHCP flow*
  - *Redirected Web server defined by administrator*
  - *(Optional) HTTP Proxy Server's IP Address*
  - *(Optional) The IP address of Server to download some applications*

  → *All the above flows are from/to wireless users*

Denied Rules

- Traffic Flows that Administrator does not intend to allow on the WLAN
- APC makes a redirection for HTTP get message only when the packet is matched by ACL denied rule.

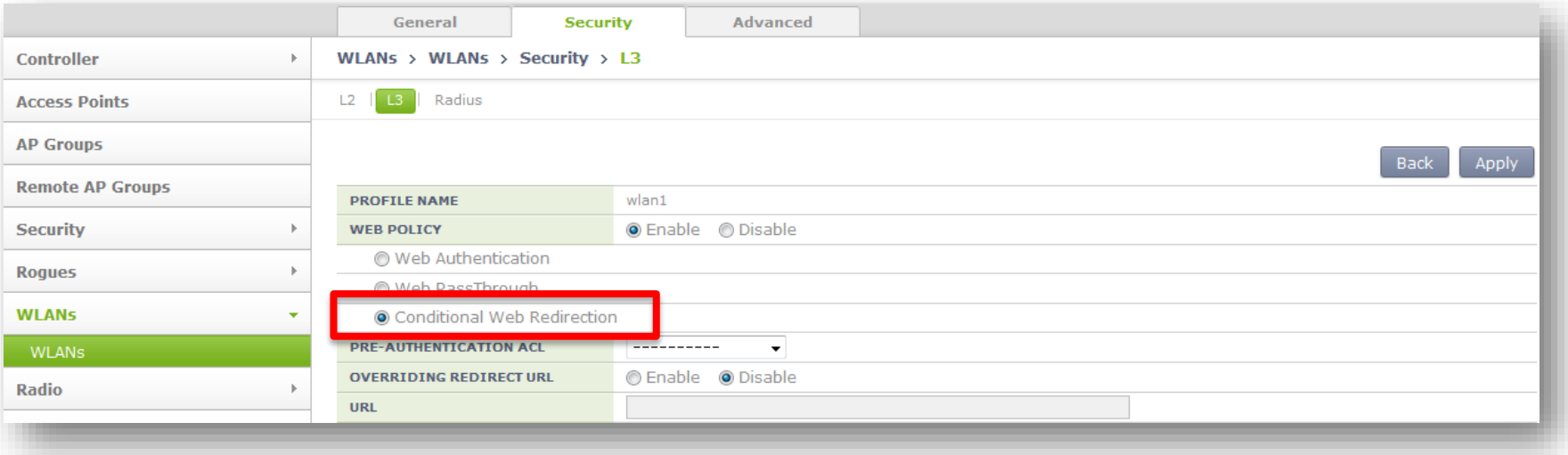
(Internal implementation!)



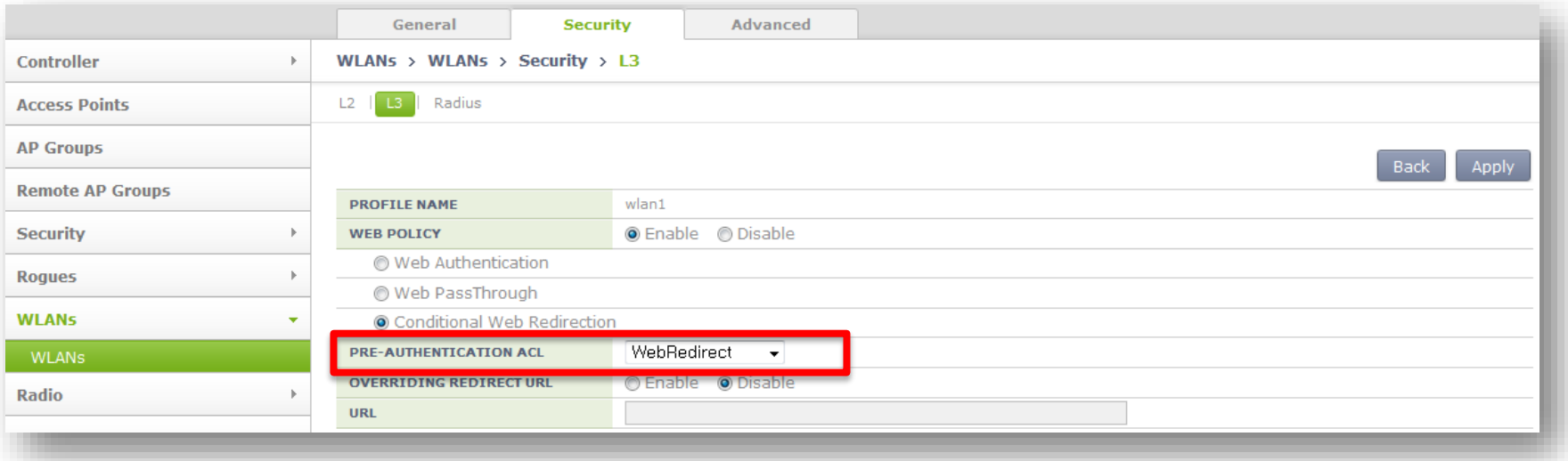
4.4.3 Setup Conditional Web Redirect

Samsung Wireless Enterprise™

Case 1 : ACL rule is referred by Samsung-Url-Redirect-Acl



Case 2 : Pre-auth-ACL is applied (Available after v1.5.0)



End of Day 2