



## Verifying the Configuration

This chapter provides the output of **show** commands that help you verify the configuration.

- [Verifying the AP Filter Configuration](#) , on page 1
- [Verifying the WLAN configuration](#), on page 2
- [Verifying the RLAN Configuration](#), on page 7

## Verifying the AP Filter Configuration

The following **show** commands are used to display tag sources and filters, and their priorities.

To view the tag source priorities, use the following command:

```
Device# show ap tag sources
```

```
Priority Tag source
-----
0 Static
1 Filter
2 AP
3 Default
```

To view the available filters, use the following command:

```
Device# show ap filter all
```

Filter Name	regex	Policy Tag	RF Tag	Site
first	abcd	pol-tag1	rf-tag1	
site-tag1				
test1	testany			site1
filter1	testany			

To view the list of active filters, use the following command:

```
Device# show ap filters active
```

Priority	Filter Name	regex	Policy Tag	RF Tag
10	test1	testany		

```
sitel
```

To view the source of an AP tag, use the following command:

```
Device# show ap tag summary
```

```
Number of APs: 4
```

AP Name	AP Mac	Site Tag Name	Policy Tag Name	RF Tag Name	Misconfigured Tag Source
AP002A.1034.CA78	002a.1034.ca78	named-site-tag	named-policy-tag	named-rf-tag	No Filter
AP00A2.891C.2480	00a2.891c.2480	named-site-tag	named-policy-tag	named-rf-tag	No Filter
AP58AC.78DE.9946	58ac.78de.9946	default-site-tag	default-policy-tag	default-rf-tag	No AP
AP0081.C4F4.1F34	0081.c4f4.1f34	default-site-tag	default-policy-tag	default-rf-tag	No Default

## Verifying the WLAN configuration

To verify the list of all WLANs configured on the controller, use the following command:

```
Device# show wlan summary
```

```
Number of WLANs: 4
```

WLAN Profile Name	SSID	VLAN	Status
1 test1	test1-ssid	137	UP
3 test2	test2-ssid	136	UP
2 test3	test3-ssid	1	UP
45 test4	test4-ssid	1	DOWN

To use wild cards and search for WLANs, use the following command:

```
Device# show wlan summary | include test-wlan-ssid
```

1	test-wlan	test-wlan-ssid	137	UP
---	-----------	----------------	-----	----

To verify the WLAN properties based on the WLAN ID, use the following command:

```
Device# show wlan id 2
```

```
WLAN Profile Name      : name
=====
Identifier              : 2
Description             :
Network Name (SSID)    : name
Status                 : Disabled
Broadcast SSID         : Enabled
Advertise-Apname       : Disabled
Universal AP Admin     : Disabled
Max Associated Clients per WLAN : 0
Max Associated Clients per AP per WLAN : 0
Max Associated Clients per AP Radio per WLAN : 200
OKC                    : Enabled
Number of Active Clients : 0
CHD per WLAN          : Enabled
```

```

WMM : Allowed
WiFi Direct Policy : Disabled
Channel Scan Defer Priority:
  Priority (default) : 5
  Priority (default) : 6
Scan Defer Time (msecs) : 100
Media Stream Multicast-direct : Disabled
CCX - AironetIe Support : Disabled
Peer-to-Peer Blocking Action : Disabled
Configured Radio Bands : All
Operational State of Radio Bands : All Bands Operational
DTIM period for 802.11a radio :
DTIM period for 802.11b radio :
Local EAP Authentication : Disabled
Mac Filter Authorization list name : Disabled
Mac Filter Override Authorization list name : Disabled
Accounting list name :
802.1x authentication list name : default
802.1x authorization list name : Disabled
Security
  802.11 Authentication : Open System
  Static WEP Keys : Disabled
  Wi-Fi Protected Access (WPA/WPA2/WPA3) : Enabled
    WPA (SSN IE) : Disabled
    WPA2 (RSN IE) : Enabled
    MP SK : Disabled
    EasyPSK : Disabled
    AES Cipher : Enabled
    CCMP256 Cipher : Disabled
    GCMP128 Cipher : Disabled
    GCMP256 Cipher : Disabled
    Randomized GTK : Disabled
  WPA3 (WPA3 IE) : Disabled
  Auth Key Management
    802.1x : Disabled
    PSK : Disabled
    CCKM : Disabled
    FT dot1x : Disabled
    FT PSK : Disabled
    Dot1x-SHA256 : Disabled
    PSK-SHA256 : Disabled
    SAE : Disabled
    OWE : Disabled
    SUITEB-1X : Disabled
    SUITEB192-1X : Disabled
  CCKM TSF Tolerance (msecs) : 1000
  OWE Transition Mode : Disabled
  OSEN : Disabled
  FT Support : Adaptive
    FT Reassociation Timeout (secs) : 20
    FT Over-The-DS mode : Disabled
  PMF Support : Disabled
    PMF Association Comeback Timeout (secs) : 1
    PMF SA Query Time (msecs) : 200
  Web Based Authentication : Disabled
  Conditional Web Redirect : Disabled
  Splash-Page Web Redirect : Disabled
  Webauth On-mac-filter Failure : Disabled
  Webauth Authentication List Name : default
  Webauth Authorization List Name : Disabled
  Webauth Parameter Map : WLAN1_MAP
Band Select : Disabled
Load Balancing : Disabled
Multicast Buffer : Disabled

```

```

Multicast Buffers (frames)           : 0
IP Source Guard                      : Disabled
Assisted-Roaming
  Neighbor List                      : Enabled
  Prediction List                    : Disabled
  Dual Band Support                   : Disabled
IEEE 802.11v parameters
  Directed Multicast Service         : Enabled
  BSS Max Idle                       : Enabled
  Protected Mode                     : Disabled
  Traffic Filtering Service          : Disabled
  BSS Transition                     : Enabled
  Disassociation Imminent            : Disabled
  Optimised Roaming Timer (TBTTs)    : 40
  Timer (TBTTs)                     : 200
  Dual Neighbor List                 : Disabled
  WNM Sleep Mode                     : Disabled
802.11ac MU-MIMO                     : Enabled
802.11ax parameters
  802.11ax Operation Status          : Enabled
  OFDMA Downlink                    : Enabled
  OFDMA Uplink                      : Enabled
  MU-MIMO Downlink                  : Enabled
  MU-MIMO Uplink                    : Enabled
  BSS Target Wake Up Time           : Enabled
  BSS Target Wake Up Time Broadcast Support : Enabled
802.11 protocols in 2.4ghz band
  Protocol                           : dot11bg
Advanced Scheduling Requests Handling : Enabled
mDNS Gateway Status                  : Bridge
WIFI Alliance Agile Multiband       : Disabled
Device Analytics
  Advertise Support                  : Enabled
  Advertise Support for PC analytics : Enabled
  Share Data with Client             : Disabled
Client Scan Report (11k Beacon Radio Measurement)
  Request on Association              : Disabled
  Request on Roam                    : Disabled
WiFi to Cellular Steering            : Disabled
Advanced Scheduling Requests Handling : Enabled
Locally Administered Address Configuration
  Deny LAA clients                  : Disabled

```

To verify the WLAN properties based on the WLAN name, use the following command:

```
Device# show wlan name test
```

```

WLAN Profile Name      : test
=====
Identifier              : 24
Description             :
Network Name (SSID)    : test
Status                 : Disabled
Broadcast SSID         : Enabled
Advertise-Appname      : Disabled
Universal AP Admin     : Disabled
Max Associated Clients per WLAN : 0
Max Associated Clients per AP per WLAN : 0
Max Associated Clients per AP Radio per WLAN : 200
OKC                    : Enabled
Number of Active Clients : 0
CHD per WLAN           : Enabled
WMM                    : Allowed
WiFi Direct Policy     : Disabled

```

```

Channel Scan Defer Priority:
  Priority (default)           : 5
  Priority (default)           : 6
Scan Defer Time (msecs)      : 100
Media Stream Multicast-direct : Disabled
CCX - AironetIe Support      : Disabled
Peer-to-Peer Blocking Action  : Disabled
Configured Radio Bands
  2.4ghz                       : Enabled
  5ghz                         : Enabled
  Slot                         : Enabled on all slots
Operational State of Radio Bands
  2.4ghz                       : UP
  5ghz                         : UP
  Slot                         : Enabled on all slots
DTIM period for 802.11a radio :
DTIM period for 802.11b radio :
Local EAP Authentication      : Disabled
Mac Filter Authorization list name : Disabled
Mac Filter Override Authorization list name : Disabled
Accounting list name          :
802.1x authentication list name : Disabled
802.1x authorization list name : Disabled
Security
  802.11 Authentication        : Open System
  Static WEP Keys              : Disabled
  Wi-Fi Protected Access (WPA/WPA2/WPA3) : Enabled
    WPA (SSN IE)               : Disabled
    WPA2 (RSN IE)              : Enabled
      MPSK                      : Disabled
      EasyPSK                   : Disabled
      AES Cipher                : Enabled
      CCMP256 Cipher            : Disabled
      GCMP128 Cipher            : Disabled
      GCMP256 Cipher            : Disabled
      Randomized GTK            : Disabled
    WPA3 (WPA3 IE)             : Disabled
  Auth Key Management
    802.1x                      : Enabled
    PSK                         : Disabled
    CCKM                        : Disabled
    FT dot1x                    : Disabled
    FT PSK                      : Disabled
    Dot1x-SHA256                : Disabled
    PSK-SHA256                  : Disabled
    SAE                         : Disabled
    OWE                         : Disabled
    SUITEB-1X                   : Disabled
    SUITEB192-1X                : Disabled
  CCKM TSF Tolerance (msecs)   : 1000
  OWE Transition Mode          : Disabled
  OSEN                         : Disabled
  FT Support                   : Adaptive
    FT Reassociation Timeout (secs) : 20
    FT Over-The-DS mode           : Disabled
  PMF Support                   : Disabled
    PMF Association Comeback Timeout (secs) : 1
    PMF SA Query Time (msecs)     : 200
  Web Based Authentication     : Disabled
  Conditional Web Redirect     : Disabled
  Splash-Page Web Redirect     : Disabled
  Webauth On-mac-filter Failure : Disabled
  Webauth Authentication List Name : Disabled
  Webauth Authorization List Name : Disabled

```

```

Webauth Parameter Map           : Disabled
Band Select                     : Disabled
Load Balancing                  : Disabled
Multicast Buffer                 : Disabled
Multicast Buffers (frames)     : 0
IP Source Guard                 : Disabled
Assisted-Roaming
  Neighbor List                 : Enabled
  Prediction List              : Disabled
  Dual Band Support            : Disabled
IEEE 802.11v parameters
  Directed Multicast Service    : Enabled
  BSS Max Idle                 : Enabled
  Protected Mode               : Disabled
  Traffic Filtering Service     : Disabled
  BSS Transition               : Enabled
  Disassociation Imminent      : Disabled
  Optimised Roaming Timer (TBTS) : 40
  Timer (TBTS)                 : 200
  Dual Neighbor List           : Disabled
WNM Sleep Mode                  : Disabled
802.11ac MU-MIMO                : Enabled
802.11ax parameters
  802.11ax Operation Status    : Enabled
  OFDMA Downlink               : Enabled
  OFDMA Uplink                 : Enabled
  MU-MIMO Downlink             : Enabled
  MU-MIMO Uplink               : Enabled
  BSS Target Wake Up Time      : Enabled
  BSS Target Wake Up Time Broadcast Support : Enabled
802.11 protocols in 2.4ghz band
  Protocol                     : dot11bg
Advanced Scheduling Requests Handling : Enabled
mDNS Gateway Status            : Bridge
WIFI Alliance Agile Multiband  : Disabled
Device Analytics
  Advertise Support            : Enabled
  Advertise Support for PC analytics : Enabled
  Share Data with Client       : Disabled
Client Scan Report (11k Beacon Radio Measurement)
  Request on Association       : Disabled
  Request on Roam              : Disabled
WiFi to Cellular Steering      : Disabled
Advanced Scheduling Requests Handling : Enabled
Locally Administered Address Configuration
  Deny LAA clients            : Disabled

```

To verify the WLAN properties of all the configured WLANs, use the following command:

```
Device# show wlan all
```

To verify the summary of all WLANs, use the following command:

```
Device# show wlan summary
```

To verify the running configuration of a WLAN based on the WLAN name, use the following command:

```
Device# show running-config wlan wlan-name
```

To verify the running configuration of all WLANs, use the following `show` command:

```

Device# show running-config wlan

wlan name 2 name
  no security wpa akm dot1x
  security dot1x authentication-list default
  security web-auth authentication-list default
  security web-auth parameter-map WLAN1_MAP
wlan test 24 test
  ip access-group web user_v4_acl
  radio policy dot11 24ghz
  radio policy dot11 5ghz
wlan test2 15 test2
wlan test4 12 testssid
  radio policy dot11 5ghz
  slot 1
  slot 2
wlan wlan1 234 wlan1
wlan wlan2 14 wlan-aaa
  security dot1x authentication-list realm
wlan wlan7 27 wlan7
wlan test23 17 test23
wlan wlan_1 4 ssid_name
  security dot1x authentication-list authenticate_list_name
wlan wlan_3 5 ssid_3
  security wpa wpa1
  security wpa wpa1 ciphers aes
wlan wlan_8 9 ssid_name
  no security wpa wpa2 ciphers aes
  no security wpa akm dot1x
  security web-auth
wlan test400 18 test_ssid
wlan testtest 45 ssid-test
wlan wlan-new 3 ssid-new
wlan local_ewa 67 local_ewa
  ip access-group web EWA_ACL
wlan test-wlan 23 test-wlan
wlan wlan-test 1 wlan2
  mac-filtering default
wlan wlan-test2 25 ssid-test3
wlan WLAN_LWA_LOCAL 35 WLAN_LWA_LOCAL
wlan wlan_lwa_local 34 wlan_lwa_local
  security web-auth authentication-list WIRELESS_LWA_AUTHENTICATION

```

## Verifying the RLAN Configuration

To view the summary of all RLANs, use the following command:

```
Device# show remote-lan summary
```

```
Number of RLANs: 1
```

RLAN	Profile Name	Status
1	rlan_test_1	Enabled

To view the RLAN configuration by ID, use the following command:

```
Device# show remote-lan id <id>
```

```
Remote-LAN Profile Name          : rlan_test_1
=====
```

```

Identifier                : 1
Status                   : Enabled
Mac-filtering             : Not Configured
Number of Active Clients  : 1
Security_8021X            : Disabled
8021.x Authentication list name : Not Configured
Local Auth eap Profile Name : Not Configured
Web Auth Security        : Disabled
Webauth Authentication list name : Not Configured
Web Auth Parameter Map   : Not Configured
Client association limit  : 0
Ipv4 Web Pre Auth Acl    : Not Configured
Ipv6 Web Pre Auth Acl    : Not Configured

```

To view the RLAN configuration by profile name, use the following command:

```
Device# show remote-lan name <profile-name>
```

```

Remote-LAN Profile Name      : rlan_test_1
=====
Identifier                   : 1
Status                       : Enabled
Mac-filtering                : Not Configured
Number of Active Clients     : 1
Security_8021X               : Disabled
8021.x Authentication list name : Not Configured
Local Auth eap Profile Name  : Not Configured
Web Auth Security            : Disabled
Webauth Authentication list name : Not Configured
Web Auth Parameter Map       : Not Configured
Client association limit     : 0
Ipv4 Web Pre Auth Acl        : Not Configured
Ipv6 Web Pre Auth Acl        : Not Configured

```

To view the detailed output of all RLANs, use the following command:

```
Device# show remote-lan all
```

```

Remote-LAN Profile Name      : rlan_test_1
=====
Identifier                   : 1
Status                       : Enabled
Mac-filtering                : Not Configured
Number of Active Clients     : 1
Security_8021X               : Disabled
8021.x Authentication list name : Not Configured
Local Auth eap Profile Name  : Not Configured
Web Auth Security            : Disabled
Webauth Authentication list name : Not Configured
Web Auth Parameter Map       : Not Configured
Client association limit     : 0
Ipv4 Web Pre Auth Acl        : Not Configured
Ipv6 Web Pre Auth Acl        : Not Configured

Remote-LAN Profile Name      : rlan_test_2
=====
Identifier                   : 2
Status                       : Enabled
Mac-filtering                : Not Configured
Number of Active Clients     : 1
Security_8021X               : Disabled
8021.x Authentication list name : Not Configured
Local Auth eap Profile Name  : Not Configured
Web Auth Security            : Disabled
Webauth Authentication list name : Not Configured

```



```

Web Auth Parameter Map           : Not Configured
Client association limit         : 0
Ipv4 Web Pre Auth Acl           : Not Configured
Ipv6 Web Pre Auth Acl           : Not Configured

```

To view the summary of policy profile for all RLANs, use the following command:

```
Device# show remote-lan policy summary
```

```
Number of Policy Profiles: 1
```

Profile Name	Description	Status
rlan_named_pp1	Testing RLAN policy profile	Enabled

To view the LAN port configuration of a Cisco AP, use the following command:

```
Device# show ap name <ap_name> lan port summary
```

```

LAN Port status for AP L2_1815w_1
Port ID      status      vlanId      poe
-----
LAN1         Enabled      20          Disabled
LAN2         Enabled      20          NA
LAN3         Disabled     0           NA

```

To view the summary of all clients, use the following command:

```
Device# show wireless client summary
```

```
Number of Local Clients: 1
```

MAC Address	AP Name	WLAN	State	Protocol	Method	Role
d8eb.97b6.fcc6	L2_1815w_1	1	* Run	Ethernet	None	Local

To view the client details with the specified username, use the following command:

```
Device# show wireless client username cisco
```

MAC Address	AP Name	Status	WLAN	Auth Protocol
0014.d1da.a977	L2_1815w_1	Run 1 *	Yes	Ethernet
d8eb.97b6.fcc6	L2_1815w_1	Run 1 *	Yes	Ethernet

To view the detailed information for a client by MAC address, use the following command:

```
Device# show wireless client mac-address <mac_address> detail
```

```

Client MAC Address : d8eb.97b6.fcc6
Client IPv4 Address : 10.2.20.78
Client IPv6 Addresses : 2001:DB8::1
Client Username: N/A
AP MAC Address : 707d.b99e.c2e0
AP Name: L2_1815w_1
AP slot : 2
Client State : Associated
Policy Profile : rlan_named_pp1
Flex Profile : rlan-flex-profile
Remote LAN Id : 1
Remote LAN Name: rlan_test_1
BSSID : 707d.b99e.c2e1
Connected For : 1159 seconds

```

```

Protocol : Ethernet
Channel : 0
Port ID: 2
Client IIF-ID : 0xa0000001
Association Id : 1
Authentication Algorithm : Open System
Client CCX version : No CCX support
Session Timeout : 1800 sec (Remaining time: 641 sec)
Input Policy Name : None
Input Policy State : None
Input Policy Source : None
Output Policy Name : None
Output Policy State : None
Output Policy Source : None
WMM Support : Disabled
Fastlane Support : Disabled
Power Save : OFF
Current Rate : 0.0
Mobility:
  Move Count : 0
  Mobility Role : Local
  Mobility Roam Type : None
  Mobility Complete Timestamp : 07/06/2018 11:25:26 IST
Policy Manager State: Run
NPU Fast Fast Notified : No
Last Policy Manager State : IP Learn Complete
Client Entry Create Time : 1159 seconds
Policy Type : N/A
Encryption Cipher : None
Encrypted Traffic Analytics : No
Management Frame Protection : No
Protected Management Frame - 802.11w : No
EAP Type : Not Applicable
VLAN : 20
Access VLAN : 20
Anchor VLAN : 0
WFD capable : No
Managed WFD capable : No
Cross Connection capable : No
Support Concurrent Operation : No
Session Manager:
  Interface : capwap_90000008
  IIF ID : 0x90000008
  Authorized : TRUE
  Session timeout : 1800
  Common Session ID: 32130209000000136C48A29D
  Acct Session ID : 0x00000000
  Aaa Server Details
  Server IP :
  Auth Method Status List
  Method : None
Local Policies:
  Service Template : wlan_svc_rlan_named_pp1_local (priority 254)
  Absolute-Timer : 1800
  VLAN : 20
Server Policies:
Resultant Policies:
  VLAN : 20
  Absolute-Timer : 1800
DNS Snooped IPv4 Addresses : None
DNS Snooped IPv6 Addresses : None
Client Capabilities
  CF Pollable : Not implemented
  CF Poll Request : Not implemented

```

```

Short Preamble : Not implemented
PECC : Not implemented
Channel Agility : Not implemented
Listen Interval : 0
Fast BSS Transition Details :
  Reassociation Timeout : 0
11v BSS Transition : Not implemented
FlexConnect Data Switching : Central
FlexConnect Dhcp Status : Central
FlexConnect Authentication : Central
FlexConnect Central Association : No
Client Statistics:
  Number of Bytes Received : 6855
  Number of Bytes Sent : 1640
  Number of Packets Received : 105
  Number of Packets Sent : 27
  Number of Policy Errors : 0
  Radio Signal Strength Indicator : 0 dBm
  Signal to Noise Ratio : 0 dB
Fabric status : Disabled
Client Scan Reports
Assisted Roaming Neighbor List
    
```

To view the summary of all AP tags, use the following command:

```
Device# show ap tag summary
```

```
Number of APs: 2
```

AP Name Tag Name	AP Mac Misconfigured	Site Tag Name Tag Source	Policy Tag Name	RF
L2_1810d_1	0008.3296.24c0	default-site-tag	default-policy-tag	
default-rf-tag	No	Default		
L2_1810w_2	00b0.e18c.5880	rlan-site-tag	rlan_pt_1	
default-rf-tag	No	Static		

To view the summary of all policy tags, use the following command:

```
Device# show wireless tag policy summary
```

```
Number of Policy Tags: 2
```

Policy Tag Name	Description
rlan_pt_1	
default-policy-tag	default policy-tag

To view details of a specific policy tag, use the following command:

```
Device# show wireless tag policy detailed <rlan_policy_tag_name>
```

```
Policy Tag Name : rlan_pt_1
Description      :
```

```
Number of WLAN-POLICY maps: 0
```

```
Number of RLAN-POLICY maps: 2
```

REMOTE-LAN Profile Name	Policy Name	Port Id
rlan_test_1	rlan_named_ppl	1

`rlan_test_1``rlan_named_pp1`

2