



## WLAN Commands

---

- [aaa-override, page 3](#)
- [accounting-list, page 4](#)
- [assisted-roaming, page 5](#)
- [band-select, page 7](#)
- [broadcast-ssid, page 8](#)
- [call-snoop, page 9](#)
- [channel-scan defer-priority, page 11](#)
- [channel-scan defer-time, page 12](#)
- [chd, page 13](#)
- [client association limit, page 14](#)
- [client vlan, page 16](#)
- [ccx aironet-iesupport, page 17](#)
- [datalink flow monitor, page 18](#)
- [default, page 20](#)
- [dtim dot11, page 23](#)
- [exclusionlist, page 24](#)
- [exit, page 25](#)
- [exit \(WLAN AP Group\), page 26](#)
- [ip access-group, page 27](#)
- [ip flow monitor, page 28](#)
- [ip verify source mac-check, page 29](#)
- [load-balance, page 30](#)
- [mobility anchor, page 31](#)
- [nac, page 33](#)

- [passive-client](#), page 34
- [peer-blocking](#), page 35
- [radio](#), page 37
- [radio-policy](#), page 39
- [roamed-voice-client re-anchor](#), page 41
- [security ft](#), page 42
- [security pmf](#), page 44
- [security web-auth](#), page 46
- [security wpa akm](#), page 47
- [service-policy \(WLAN\)](#), page 49
- [session-timeout](#), page 51
- [show wlan](#), page 52
- [shutdown](#), page 55
- [sip-cac](#), page 56
- [static-ip tunneling](#), page 57
- [vlan](#), page 58
- [wgb non-cisco](#), page 59
- [wifidirect policy](#), page 60
- [wlan \(AP Group Configuration\)](#), page 61
- [wlan](#), page 62
- [wlan shutdown](#), page 63
- [wmm](#), page 64

# aaa-override

To enable AAA override on the WLAN, use the **aaa-override** command. To disable AAA override, use the **no** form of this command.

**aaa-override**

**no aaa-override**

**Syntax Description** This command has no keywords or arguments.

**Command Default** AAA is disabled by default.

**Command Modes** WLAN configuration

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

**Usage Guidelines** You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

**Examples** This example shows how to enable AAA on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# shutdown
Controller(config-wlan)# aaa-override
Controller(config-wlan)# no shutdown
Controller(config-wlan)# end
```

This example shows how to disable AAA on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# shutdown
Controller(config-wlan)# no aaa-override
Controller(config-wlan)# no shutdown
Controller(config-wlan)# end
```

Command	Description
<a href="#">wlan</a>	Creates or disables a WLAN.

# accounting-list

To configure RADIUS accounting servers on a WLAN, use the **accounting-list** command. To disable RADIUS server accounting, use the **no** form of this command.

**accounting-list** *radius-server-acct*

**no accounting-list**

## Syntax Description

<i>radius-server-acct</i>	Accounting RADIUS server name.
---------------------------	--------------------------------

## Command Default

RADIUS server accounting is disabled by default.

## Command Modes

WLAN configuration

## Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

## Usage Guidelines

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

## Examples

This example shows how to configure RADIUS server accounting on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# accounting-list test
Controller(config-wlan)# end
```

This example shows how to disable RADIUS server accounting on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# no accounting-list test
Controller(config-wlan)# end
```

## Related Commands

Command	Description
<a href="#">wlan</a>	Creates or disables a WLAN.

# assisted-roaming

To configure assisted roaming using 802.11k on a WLAN, use the **assisted-roaming** command. To disable assisted roaming, use the **no** form of this command.

**assisted-roaming** {**dual-list**| **neighbor-list**| **prediction**}

**no assisted-roaming** {**dual-list**| **neighbor-list**| **prediction**}

## Syntax Description

<b>dual-list</b>	Configures a dual band 802.11k neighbor list for a WLAN. The default is the band that the client is currently associated with.
<b>neighbor-list</b>	Configures an 802.11k neighbor list for a WLAN.
<b>prediction</b>	Configures assisted roaming optimization prediction for a WLAN.

## Command Default

Neighbor list and dual band support are enabled by default. The default is the band that the client is currently associated with.

## Command Modes

WLAN configuration

## Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

## Usage Guidelines

When you enable the assisted roaming prediction list, a warning appears and load balancing is disabled for the WLAN if load balancing is already enabled on the WLAN. To make changes to the WLAN, the WLAN must be in disabled state.

## Examples

The following example shows how to configure a 802.11k neighbor list on a WLAN:

```
Controller(config-wlan)#assisted-roaming neighbor-list
```

The following example shows the warning message when load balancing is enabled on a WLAN. Load balancing must be disabled if it is already enabled when configuring assisted roaming:

```
Controller(config)#wlan test-prediction 2 test-prediction
Controller(config-wlan)#client vlan 43
Controller(config-wlan)#no security wpa
Controller(config-wlan)#load-balance
Controller(config-wlan)#assisted-roaming prediction
WARNING: Enabling neighbor list prediction optimization may slow association and impact
VOICE client perform.
Are you sure you want to continue? (y/n)[y]: y
```

% Request aborted - Must first disable Load Balancing before enabling Assisted Roaming Prediction Optimization on this WLAN.

# band-select

To configure band selection on a WLAN, use the **band-select** command. To disable band selection, use the **no** form of this command.

**band-select**

**no band-select**

**Syntax Description** This command has no keywords or arguments.

**Command Default** Band selection is disabled by default.

**Command Modes** WLAN configuration

Command History	Release	Modification
	Cisco IOS XE 3.2SE	This command was introduced.

**Usage Guidelines** When you enable band select on a WLAN, the access point suppresses client probes on 2.4GHz and moves the dual band clients to the 5-GHz spectrum. The band-selection algorithm directs dual-band clients only from the 2.4-GHz radio to the 5-GHz radio of the same access point, and it only runs on an access point when both the 2.4-GHz and 5-GHz radios are up and running.

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

**Examples** This example shows how to enable band select on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# band-select
Controller(config-wlan)# end
```

This example shows how to disable band selection on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# no band-select
Controller(config-wlan)# end
```

Related Commands	Command	Description
	<a href="#">wlan</a>	Creates or disables a WLAN.

# broadcast-ssid

To enable a Service Set Identifier (SSID) on a WLAN, use the **broadcast-ssid** command. To disable broadcasting of SSID, use the **no** form of this command.

**broadcast-ssid**

**no broadcast-ssid**

## Syntax Description

This command has no keywords or arguments.

## Command Default

The SSIDs of WLANs are broadcasted by default.

## Command Modes

WLAN configuration

## Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

## Usage Guidelines

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

## Examples

This example shows how to enable a broadcast SSID on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# broadcast-ssid
Controller(config-wlan)# end
```

This example shows how to disable a broadcast SSID on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# no broadcast-ssid
Controller(config-wlan)# end
```

## Related Commands

Command	Description
<a href="#">wlan</a>	Creates or disables a WLAN.



# call-snoop

To enable Voice over IP (VoIP) snooping on a WLAN, use the **call-snoop** command. To disable Voice over IP (VoIP), use the **no** form of this command.

**call-snoop**

**no call-snoop**

**Syntax Description** This command has no keywords or arguments.

**Command Default** VoIP snooping is disabled by default.

**Command Modes** WLAN configuration

**Usage Guidelines** You must disable the WLAN before using this command. See the Related Commands section for more information on how to disable a WLAN.

Command History	Release	Modification
	Cisco IOS XE 3.2SE	This command was introduced.

**Usage Guidelines** The WLAN on which call snooping is configured must be configured with Platinum QoS. You must disable quality of service before using this command. See Related Commands section for more information on configuring QoS service-policy.

**Examples** This example shows how to enable VoIP on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# call-snoop
Controller(config-wlan)# end
```

This example shows how to disable VoIP on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# no call-snoop
Controller(config-wlan)# end
```

Related Commands	Command	Description
	<a href="#">service-policy (WLAN)</a>	Configures the QoS Policy on a WLAN.

Command	Description
<a href="#">wlan</a>	Creates or disables a WLAN.

## channel-scan defer-priority

To configure the device to defer priority markings for packets that can defer off-channel scanning, use the **channel-scan defer-priority** command. To disable the device to defer priority markings for packets that can defer off-channel scanning, use the **no** form of this command.

**channel-scan defer-priority** *priority*

**no channel-scan defer-priority** *priority*

<b>Syntax Description</b>	<i>priority</i>	Channel priority value. The range is 0 to 7. The default is 3.
<b>Command Default</b>	Channel scan defer is enabled.	
<b>Command Modes</b>	WLAN configuration	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE 3.2SE	This command was introduced.

### Examples

This example shows how to enable channel scan defer priority on a WLAN and set it to a priority value 4:

```
Controller# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# channel-scan defer-priority 4
Controller(config-wlan)# end
```

This example shows how to disable channel scan defer priority on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# no channel-scan defer-priority 4
Controller(config-wlan)# end
```

# channel-scan defer-time

To assign a channel scan defer time, use the **channel-scan defer-time** command. To disable the channel scan defer time, use the **no** form of this command.

**channel-scan defer-time** *msecs*

**no channel-scan defer-time**

## Syntax Description

<i>msecs</i>	Deferral time in milliseconds. The range is from 0 to 60000. The default is 100.
--------------	--

## Command Default

Channel-scan defer time is enabled.

## Command Modes

WLAN configuration

## Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

## Usage Guidelines

The time value in milliseconds should match the requirements of the equipment on the WLAN.

## Examples

This example shows how to enable a channel scan on the WLAN and set the scan deferral time to 300 milliseconds:

```
Controller# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# channel-scan defer-time 300
Controller(config-wlan)# end
```

This example shows how to disable channel scan defer time on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# no channel-scan defer-time
Controller(config-wlan)# end
```

# chd

To enable coverage hole detection on a WLAN, use the **chd** command. To disable coverage hole detection, use the **no** form of this command.

**chd**

**no chd**

**Syntax Description** This command has no keywords or arguments.

**Command Default** Coverage hole detection is enabled.

**Command Modes** WLAN configuration

Command History	Release	Modification
	Cisco IOS XE 3.2SE	This command was introduced.

## Examples

This example shows how to enable coverage hole detection on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# chd
Controller(config-wlan)# end
```

This example shows how to disable coverage hole detection on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# no chd
Controller(config-wlan)# end
```

# client association limit

To configure the maximum number of client connections, clients per access points, or clients per access point radio on a WLAN, use the **client association limit** command. To disable clients on the WLAN, use the **no** form of this command.

**client association limit** {*association-limit*| **ap** *ap-limit*| **radio** *max-ap-radio-limit*}

**no client association limit** {*association-limit*| **ap** *ap-limit*| **radio** *max-ap-radio-limit*}

## Syntax Description

<i>association-limit</i>	Number of client connections to be accepted. The range is from 0 to 12000. A value of zero (0) indicates no set limit.
<b>ap</b>	Maximum number of clients per access point.
<i>ap-limit</i>	Configures the maximum number of client connections to be accepted per access point radio. The valid range is from 0 to 400.
<b>radio</b>	Configures the maximum number of clients per AP radio.
<i>max-ap-radio-limit</i>	Maximum number of client connections to be accepted per access point radio. The valid range is from 0 - 200.

## Command Default

The maximum number of client connections is set to 0 (no limit).

## Command Modes

WLAN configuration

## Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.
Cisco IOS XE 3.3SE	The command was modified. The <b>ap</b> and <b>radio</b> keywords were added.

**Usage Guidelines**

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

**Examples**

This example shows how to configure a client association limit on a WLAN and configure the client limit to 200:

```
Controller# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# shutdown
Controller(config-wlan)# client association limit 200
Controller(config-wlan)# no shutdown
Controller(config-wlan)# end
```

This example shows how to disable a client association limit on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# shutdown
Controller(config-wlan)# no client association limit
Controller(config-wlan)# no shutdown
Controller(config-wlan)# end
```

This example shows how to configure a client association limit per radio on a WLAN and configure the client limit to 200:

```
Controller# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# client association limit radio 200
Controller(config-wlan)# no shutdown
Controller(config-wlan)# end
```

This example shows how to configure a client association limit per AP on a WLAN and configure the client limit to 300::

```
Controller# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# client association limit ap 300
Controller(config-wlan)# no shutdown
Controller(config-wlan)# end
```

**Related Commands**

Command	Description
<a href="#">wlan</a>	Creates or disables a WLAN.

# client vlan

To configure a WLAN interface or an interface group, use the **client vlan** command. To disable the WLAN interface, use the **no** form of this command.

**client vlan** *interface-id-name-or-group-name*

**no client vlan**

## Syntax Description

<i>interface--id-name-or-group-name</i>	Interface ID, name, or VLAN group name.
---	---

## Command Default

The default interface is configured.

## Command Modes

WLAN configuration

## Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

## Usage Guidelines

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

## Examples

This example shows how to enable a client VLAN on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# client vlan client-vlan1
Controller(config-wlan)# end
```

This example shows how to disable a client association limit on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# no client vlan
Controller(config-wlan)# end
```

## Related Commands

Command	Description
<a href="#">wlan</a>	Creates or disables a WLAN.



# ccx aironet-iesupport

To enable Aironet Information Elements (IEs) for a WLAN, use the **ccx aironet-iesupport** command. To disable Aironet Information Elements (IEs), use the **no** form of this command.

**ccx aironet-iesupport**

**no ccx aironet-iesupport**

**Syntax Description** This command has no keywords or arguments.

**Command Default** Aironet IE support is enabled.

**Command Modes** WLAN configuration

Command History	Release	Modification
	Cisco IOS XE 3.2SE	This command was introduced.

**Usage Guidelines** You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

**Examples** This example shows how to enable an Aironet IE for a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# ccx aironet-iesupport
Controller(config-wlan)# end
```

This example shows how to disable an Aironet IE on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# no ccx aironet-iesupport
Controller(config-wlan)# end
```

Related Commands	Command	Description
	<a href="#">wlan</a>	Creates or disables a WLAN.

# datalink flow monitor

To enable NetFlow monitoring in a WLAN, use the **datalink flow monitor** command. To disable NetFlow monitoring, use the **no** form of this command.

**datalink flow monitor** *datalink-monitor-name* {**input**|**output**}

**no datalink flow monitor** *datalink-monitor-name* {**input**|**output**}

## Syntax Description

<i>datalink-monitor-name</i>	Flow monitor name. The datalink monitor name can have up to 31 characters.
<b>input</b>	Specifies the NetFlow monitor for ingress traffic.
<b>output</b>	Specifies the NetFlow monitor for egress traffic.

## Command Default

None.

## Command Modes

WLAN configuration

## Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

## Usage Guidelines

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

## Examples

This example shows how to enable NetFlow monitoring on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# datalink flow monitor test output
Controller(config-wlan)# end
```

This example shows how to disable NetFlow monitoring on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# no datalink flow monitor test output
Controller(config-wlan)# end
```

**Related Commands**

Command	Description
<a href="#">wlan</a>	Creates or disables a WLAN.

# default

To set the parameters to their default values, use the **default** command.

**default** {aaa-override| accounting-list| band-select| broadcast-ssid| call-snoop| ccx| channel-scan| parameters| chd| client| datalink| diag-channel| dtim| exclusionlist| ip| ipv6| load-balance| local-auth| mac-filtering| media-stream| mfp| mobility| nac| passive-client| peer-blocking| radio| roamed-voice-client| security| service-policy| session-timeout| shutdown| sip-cac| static-ip| uapsd| wgb| wmm}

## Syntax Description

<b>aaa-override</b>	Sets the AAA override parameter to its default value.
<b>accounting-list</b>	Sets the accounting parameter and its attributes to their default values.
<b>band-select</b>	Sets the band selection parameter to its default values.
<b>broadcast-ssid</b>	Sets the broadcast Service Set Identifier (SSID) parameter to its default value.
<b>call-snoop</b>	Sets the call snoop parameter to its default value.
<b>ccx</b>	Sets the Cisco client extension (Cisco Aironet IE) parameters and attributes to their default values.
<b>channel-scan</b>	Sets the channel scan parameters and attributes to their default values.
<b>chd</b>	Sets the coverage hold detection parameter to its default value.
<b>client</b>	Sets the client parameters and attributes to their default values.
<b>datalink</b>	Sets the datalink parameters and attributes to their default values.
<b>diag-channel</b>	Sets the diagnostic channel parameters and attributes to their default values.
<b>dtim</b>	Sets the Delivery Traffic Indicator Message (DTIM) parameter to its default value.
<b>exclusionlist</b>	Sets the client exclusion timeout parameter to its default value.
<b>ip</b>	Sets the IP parameters to their default values.
<b>ipv6</b>	Sets the IPv6 parameters and attributes to their default values.
<b>load-balance</b>	Sets the load-balancing parameter to its default value.
<b>local-auth</b>	Sets the Extensible Authentication Protocol (EAP) profile parameters and attributes to their default values.
<b>mac-filtering</b>	Sets the MAC filtering parameters and attributes to their default values.

<b>media-stream</b>	Sets the media stream parameters and attributes to their default values.
<b>mfp</b>	Sets the Management Frame Protection (MPF) parameters and attributes to their default values.
<b>mobility</b>	Sets the mobility parameters and attributes to their default values.
<b>nac</b>	Sets the RADIUS Network Admission Control (NAC) parameter to its default value.
<b>passive-client</b>	Sets the passive client parameter to its default value.
<b>peer-blocking</b>	Sets the peer to peer blocking parameters and attributes to their default values.
<b>radio</b>	Sets the radio policy parameters and attributes to their default values.
<b>roamed-voice-client</b>	Sets the roamed voice client parameters and attributes to their default values.
<b>security</b>	Sets the security policy parameters and attributes to their default values.
<b>service-policy</b>	Sets the WLAN quality of service (QoS) policy parameters and attributes to their default values.
<b>session-timeout</b>	Sets the client session timeout parameter to its default value.
<b>shutdown</b>	Sets the shutdown parameter to its default value.
<b>sip-cac</b>	Sets the Session Initiation Protocol (SIP) Call Admission Control (CAC) parameters and attributes to their default values.
<b>static-ip</b>	Sets the static IP client tunneling parameters and their attributes to their default values.
<b>uapsd</b>	Sets the Wi-Fi Multimedia (WMM) Unscheduled Automatic Power Save Delivery (UAPSD) parameters and attributes to their default values.
<b>wgb</b>	Sets the Workgroup Bridges (WGB) parameter to its default value.
<b>wmm</b>	Sets the WMM parameters and attributes to their default values.

**Command Default**

None.

**Command Modes**

WLAN configuration

**Command History**

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

**Usage Guidelines**

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

**Examples**

This example shows how to set the Cisco Client Extension parameter to its default value:

```
Controller(config-wlan) # default ccx aironet-iesupport
```

**Related Commands**

Command	Description
<a href="#">wlan</a>	Creates or disables a WLAN.

# dtim dot11

To configure the Delivery Traffic Indicator Message (DTIM) period for a WLAN, use the **dtim dot11** command. To disable DTIM, use the **no** form of this command.

**dtim dot11** {5ghz| 24ghz} *dtim-period*

**no dtim dot11** {5ghz| 24ghz} *dtim-period*

## Syntax Description

<b>5ghz</b>	Configures the DTIM period on the 5-GHz band.
<b>24ghz</b>	Configures the DTIM period on the 2.4-GHz band.
<i>dtim-period</i>	Value for the DTIM period. The range is from 1 to 255.

## Command Default

The DTIM period is set to 1.

## Command Modes

WLAN configuration

## Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

## Usage Guidelines

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

## Examples

This example shows how to enable the DTIM period on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# dtim dot11 24ghz 3
```

This example shows how to disable the DTIM period on a WLAN on the 2.4-GHz band:

```
Controller# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# no dtim dot11 24ghz 3
```

## Related Commands

Command	Description
<a href="#">wlan</a>	Creates or disables a WLAN.

# exclusionlist

To configure an exclusion list on a wireless LAN, use the **exclusionlist** command. To disable an exclusion list, use the **no** form of this command.

**exclusionlist** [*timeout seconds*]

**no exclusionlist** [*timeout*]

## Syntax Description

<b>timeout</b> <i>seconds</i>	(Optional) Specifies an exclusion list timeout in seconds. The range is from 0 to 2147483647. A value of zero (0) specifies no timeout.
-------------------------------	---

## Command Default

The exclusion list is set to 60 seconds.

## Command Modes

WLAN configuration

## Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

## Usage Guidelines

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

## Examples

This example shows how to configure a client exclusion list for a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# exclusionlist timeout 345
```

This example shows how to disable a client exclusion list on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# no exclusionlist timeout 345
```



# exit

To exit the WLAN configuration submode, use the **exit** command.

**exit**

<b>Syntax Description</b>	This command has no keywords or arguments.
---------------------------	--

<b>Command Default</b>	None
------------------------	------

<b>Command Modes</b>	WLAN configuration
----------------------	--------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE 3.2SE	This command was introduced.

**Examples** This example shows how to exit the WLAN configuration submode:

```
Controller# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# exit
Controller(config)#
```

## exit (WLAN AP Group)

To exit the WLAN access point group submode, use the **exit** command.

**exit**

<b>Syntax Description</b>	This command has no keywords or arguments.
---------------------------	--

<b>Command Default</b>	None
------------------------	------

<b>Command Modes</b>	WLAN AP Group configuration
----------------------	-----------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE 3.2SE	This command was introduced.

**Examples** This example shows how to exit the WLAN AP group submode:

```
Controller# configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
Controller(config)# ap group test  
Controller(config-apgroup)# exit
```

# ip access-group

To configure WLAN access control group (ACL), use the **ip access-group** command. To remove a WLAN ACL group, use the **no** form of the command.

**ip access-group [web] *acl-name***

**no ip access-group [web]**

## Syntax Description

<b>web</b>	(Optional) Configures the IPv4 web ACL.
<i>acl-name</i>	Specify the preauth ACL used for the WLAN with the security type value as webauth.

## Command Default

None

## Command Modes

WLAN configuration

## Usage Guidelines

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

## Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

## Examples

This example shows how to configure a WLAN ACL:

```
Controller#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Controller(config)#wlan wlan1
Controller(config-wlan)#ip access-group test-acl
```

This example shows how to configure an IPv4 WLAN web ACL:

```
Controller# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# ip access-group web test
Controller(config-wlan)#
```

## Related Commands

Command	Description
<a href="#">wlan</a>	Creates or disables a WLAN.

# ip flow monitor

To configure IP NetFlow monitoring, use the **ip flow monitor** command. To remove IP NetFlow monitoring, use the **no** form of this command.

**ip flow monitor** *ip-monitor-name* {**input**|**output**}

**no ip flow monitor** *ip-monitor-name* {**input**|**output**}

## Syntax Description

<i>ip-monitor-name</i>	Flow monitor name.
<b>input</b>	Enables a flow monitor for ingress traffic.
<b>output</b>	Enables a flow monitor for egress traffic.

## Command Default

None

## Command Modes

WLAN configuration

## Usage Guidelines

You must disable the WLAN before using this command.

## Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

## Examples

This example shows how to configure an IP flow monitor for the ingress traffic:

```
Controller# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# ip flow monitor test input
```

This example shows how to disable an IP flow monitor:

```
Controller# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# no ip flow monitor test input
```

# ip verify source mac-check

To enable IPv4 Source Guard (IPSG) on a WLAN, use the **ip verify source mac-check** command. To disable IPSG, use the **no** form of this command.

**ip verify source mac-check**

**no ip verify source mac-check**

**Syntax Description** This command has no keywords or arguments.

**Command Default** IPSG is disabled.

**Command Modes** WLAN configuration

Command History	Release	Modification
	Cisco IOS XE 3.2SE	This command was introduced.

**Usage Guidelines** Use this feature to restrict traffic from a host to a specific interface that is based on the host's IP address. The feature can also be configured to bind the source MAC and IP of a host so that IP spoofing is prevented.

Use this feature to bind the IP and MAC address of a wireless host that is based on information received from DHCP snooping, ARP, and Dataglean. Dataglean is the process of extracting location information such as host hardware address, ports that lead to the host, and so on from DHCP messages as they are forwarded by the DHCP relay agent. If a wireless host tries to send traffic with IP address and MAC address combination that has not been learned by the controller, this traffic is dropped in the hardware. IPSG is not supported on DHCP packets. IPSG is not supported for foreign clients in a foreign controller.

You must disable the WLAN before using this command.

**Examples** This example shows how to enable IPSG:

```
Controller# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# ip verify source mac-check
```

This example shows how to disable IPSG:

```
Controller# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# no ip verify source mac-check
```

# load-balance

To enable load balancing on a WLAN, use the **load-balance** command. To disable load balancing, use the **no** form of this command.

**load-balance**

**no load-balance**

**Syntax Description** This command has no keywords or arguments.

**Command Default** Load balancing is disabled by default.

**Command Modes** WLAN configuration

Release	Modification
Cisco IOS XE 3.2SE	The command was introduced.

**Usage Guidelines** You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

**Examples** This example shows how to enable load balancing on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Controller(config)# shutdown
Controller(config)# wlan wlan1
Controller(config-wlan)# load-balance
Controller(config)# no shutdown
Controller(config-wlan)# end
```

This example shows how to disable load balancing on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Controller(config)# shutdown
Controller(config)# wlan wlan1
Controller(config-wlan)# no load-balance
Controller(config)# no shutdown
Controller(config-wlan)# end
```

Command	Description
<a href="#">wlan</a>	Creates or disables a WLAN.

# mobility anchor

To configure mobility sticky anchoring, use the **mobility anchor sticky** command. To disable the sticky anchoring, use the **no** form of the command.

To configure guest anchoring, use the **mobility anchor ip-address** command.

To delete the guest anchor, use the **no** form of the command.

To configure the device as an auto-anchor, use the **mobility anchor** command.

**mobility anchor** {*ip-address*| **sticky**}

**no mobility anchor** {*ip-address*| **sticky**}

## Syntax Description

<b>sticky</b>	The client is anchored to the first switch that it associates.
	<b>Note</b> This command is by default enabled and ensures low roaming latency. This ensures that the point of presence for the client does not change when the client joins the mobility domain and roams within the domain.
<i>ip-address</i>	Configures the IP address for the guest anchor controller to this WLAN.

## Command Default

Sticky configuration is enabled by default.

## Command Modes

WLAN Configuration

## Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.
Cisco IOS XE 3.3SE	The auto-anchor configuration required the device IP address to be entered prior to the Cisco IOS XE 3.3SE release; with this release, if no IP address is given, the device itself becomes an anchor; you do not have to explicitly specify the IP address.

## Usage Guidelines

- The `wlan_id` or `guest_lan_id` must exist and be disabled.
- Auto-anchor mobility is enabled for the WLAN or wired guest LAN when you configure the first mobility anchor.
- Deleting the last anchor disables the auto-anchor mobility feature and resumes normal mobility for new associations.
- Mobility uses the following ports, that are allowed through the firewall:

- 16666
- 16667
- 16668

## Examples

This example shows how to enable the sticky mobility anchor:

```
Controller(config-wlan) # mobility anchor sticky
```

This example shows how to configure guest anchoring:

```
Controller(config-wlan) # mobility anchor 209.165.200.224
```

This example shows how to configure the device as an auto-anchor:

```
Controller(config-wlan) # mobility anchor
```



## nac

To enable RADIUS Network Admission Control (NAC) support for a WLAN, use the **nac** command. To disable NAC out-of-band support, use the **no** form of this command.

**nac**

**no nac**

**Syntax Description** This command has no keywords or arguments.

**Command Default** NAC is disabled.

**Command Modes** WLAN configuration

Command History	Release	Modification
	Cisco IOS XE 3.2SE	This command was introduced.

**Usage Guidelines** You should enable AAA override before you enable the RADIUS NAC state.

**Examples** This example shows how to configure RADIUS NAC on the WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# aaa-override
Controller(config-wlan)# nac
```

This example shows how to disable RADIUS NAC on the WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# no nac
Controller(config-wlan)# no aaa-override
```

Related Commands	Command	Description
	<a href="#">aaa-override</a>	Enables or disables AAA override on a WLAN.

# passive-client

To enable the passive client feature on a WLAN, use the **passive-client** command. To disable the passive client feature, use the **no** form of this command.

**passive-client**

**no passive-client**

**Syntax Description** This command has no keywords or arguments.

**Command Default** Passive client feature is disabled.

**Command Modes** WLAN configuration

Command History	Release	Modification
	Cisco IOS XE 3.2SE	This command was introduced.

**Usage Guidelines** You must enable the global multicast mode and multicast-multicast mode before entering this command. Both multicast-multicast mode and multicast unicast modes are supported. The multicast-multicast mode is recommended.

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

**Examples** This show how to enable the passive client feature on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Controller(config)# wireless multicast
Controller(config)# wlan test-wlan
Controller(config-wlan)# passive-client
```

This example shows how to disable the passive client feature on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Controller(config)# wireless multicast
Controller(config)# wlan test-wlan
Controller(config-wlan)# no passive-client
```

Related Commands	Command	Description
	<a href="#">wlan</a>	Creates or disables a WLAN.

# peer-blocking

To configure peer-to-peer blocking on a WLAN, use the **peer-blocking** command. To disable peer-to-peer blocking, use the **no** form of this command.

**peer-blocking** {**drop**|**forward-upstream**}

**no peer-blocking**

## Syntax Description

<b>drop</b>	Specifies the controller to discard the packets.
<b>forward-upstream</b>	Specifies the packets to be forwarded on the upstream VLAN. The device next in the hierarchy to the controller decides what action to take regarding the packets.

## Command Default

Peer blocking is disabled.

## Command Modes

WLAN configuration

## Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

## Usage Guidelines

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

## Examples

This example shows how to enable the drop and forward-upstream options for peer-to-peer blocking:

```
Controller# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# peer-blocking drop
Controller(config-wlan)# peer-blocking forward-upstream
```

This example shows how to disable the drop and forward-upstream options for peer-to-peer blocking:

```
Controller# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# no peer-blocking drop
Controller(config-wlan)# no peer-blocking forward-upstream
```

**Related Commands**

Command	Description
<a href="#">wlan</a>	Creates or disables a WLAN.

# radio

To enable the Cisco radio policy on a WLAN, use the **radio** command. To disable the Cisco radio policy on a WLAN, use the **no** form of this command.

**radio** {all| dot11a| dot11ag| dot11bg| dot11g}

**no radio**

## Syntax Description

<b>all</b>	Configures the WLAN on all radio bands.
<b>dot11a</b>	Configures the WLAN on only 802.11a radio bands.
<b>dot11ag</b>	Configures the WLAN on 802.11a/g radio bands.
<b>dot11bg</b>	Configures the wireless LAN on only 802.11b/g radio bands (only 802.11b if 802.11g is disabled).
<b>dot11g</b>	Configures the wireless LAN on 802.11g radio bands only.

## Command Default

Radio policy is enabled on all bands.

## Command Modes

WLAN configuration

## Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

## Usage Guidelines

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

## Examples

This example shows how to configure the WLAN on all radio bands:

```
Controller# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# radio all
```

This example shows how to disable all radio bands on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# no radio all
```

**Related Commands**

Command	Description
<a href="#">wlan</a>	Creates or disables a WLAN.

# radio-policy

To configure the radio policy on a WLAN access point group, use the **radio-policy** command. To disable the radio policy on the WLAN, use the **no** form of this command.

**radio-policy** {all| dot11a| dot11bg| dot11g}

**no radio** {all| dot11a| dot11bg| dot11g}

## Syntax Description

<b>all</b>	Configures the wireless LAN on all radio bands.
<b>dot11a</b>	Configures the wireless LAN on only 802.11a radio bands.
<b>dot11bg</b>	Configures the wireless LAN on only 802.11b/g (only 802.11b if 802.11g is disabled) radio bands.
<b>dot11g</b>	Configures the wireless LAN on only 802.11g radio bands.

## Command Default

Radio policy is enabled on all the bands.

## Command Modes

WLAN AP Group configuration

## Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

## Usage Guidelines

The WLAN must be restarted for the changes to take effect. See Related Commands section for more information on how to shutdown a WLAN.

## Examples

This example shows how to enable the radio policy on the 802.11b band for an AP group:

```
Controller(config)# ap group test
Controller(config-apgroup)# wlan test-wlan
Controller(config-wlan-apgroup)# radio-policy dot11b
```

This example shows how to disable the radio policy on the 802.11b band of an AP group:

```
Controller(config)# ap group test
Controller(config-apgroup)# wlan test-wlan
Controller(config-wlan-apgroup)# no radio-policy dot11bg
```

**Related Commands**

Command	Description
<a href="#">wlan</a>	Creates or disables a WLAN.
<a href="#">wlan shutdown</a>	Disables a WLAN.



# roamed-voice-client re-anchor

To enable the roamed-voice-client re-anchor feature, use the **roamed-voice-client re-anchor** command. To disable the roamed-voice-client re-anchor feature, use the **no** form of this command.

**roamed-voice-client re-anchor**

**no roamed-voice-client re-anchor**

**Syntax Description** This command has no keywords or arguments.

**Command Default** Roamed voice client reanchor feature is disabled.

**Command Modes** WLAN configuration

Command History	Release	Modification
	Cisco IOS XE 3.2SE	This command was introduced.

**Usage Guidelines** You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

**Examples** This example shows how to enable the roamed voice client re-anchor feature:

```
Controller# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# roamed-voice-client re-anchor
```

This example shows how to disable the roamed voice client re-anchor feature:

```
Controller# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# no roamed-voice-client re-anchor
```

Related Commands	Command	Description
	<a href="#">wlan</a>	Creates or disables a WLAN.

# security ft

To configure 802.11r fast transition parameters, use the **security ft** command. To configure fast transition over the air, use the **no security ft over-the-ds** command.

**security ft** [**over-the-ds**] **reassociation-timeout** *timeout-jn-seconds*

**no security ft** [**over-the-ds**] **reassociation-timeout**

## Syntax Description

<b>over-the-ds</b>	(Optional) Specifies that the 802.11r fast transition occurs over a distributed system. The no form of the command with this parameter configures security ft over the air.
<b>reassociation-timeout</b>	(Optional) Configures the reassociation timeout interval.
<i>timeout-in-seconds</i>	(Optional) Specifies the reassociation timeout interval in seconds. The valid range is between 1 to 100. The default value is 20.

## Command Default

The feature is disabled.

## Command Modes

WLAN configuration

## Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

## Usage Guidelines

None

WLAN Security must be enabled.

## Examples

The following example configures security FT configuration for an open WLAN:

```
Controller#wlan test
Controller(config-wlan)# client vlan 0140
Controller(config-wlan)# no mobility anchor sticky
Controller(config-wlan)# no security wpa
Controller(config-wlan)# no security wpa akm dot1x
Controller(config-wlan)# no security wpa wpa2
Controller(config-wlan)# no security wpa wpa2 ciphers aes
Controller(config-wlan)# security ft
Controller(config-wlan)# shutdown
```

The following example shows a sample security FT on a WPA-enabled WLAN:

```
Controller# wlan test
```

```
Controller(config-wlan)# client vlan 0140
Controller(config-wlan)# no security wpa akm dot1x
Controller(config-wlan)# security wpa akm ft psk
Controller(config-wlan)# security wpa akm psk set-key ascii 0 test-test
Controller(config-wlan)# security ft
Controller(config-wlan)# no shutdown
```

## security pmf

To configure 802.11w Management Frame Protection (PMF) on a WLAN, use the **security pmf** command. To disable management frame protection, use the **no** form of the command.

**security pmf** {**association-comeback** *association-comeback-time-seconds*| **mandatory**| **optional**| **saquery-retry-time** *saquery-retry-time-milliseconds*}

**no security pmf** [**association-comeback** *association-comeback-time-seconds*| **mandatory**| **optional**| **saquery-retry-time** *saquery-retry-time-milliseconds*]

### Syntax Description

<b>association-comeback</b>	Configures the 802.11w association comeback time.
<i>association-comeback-time-seconds</i>	Association comeback interval in seconds. Time interval that an associated client must wait before the association is tried again after it is denied with a status code 30. The status code 30 message is "Association request rejected temporarily; Try again later."  The range is from 1 through 20 seconds.
<b>mandatory</b>	Specifies that clients are required to negotiate 802.1w PMF protection on the WLAN.
<b>optional</b>	Specifies that the WLAN does not mandate 802.11w support on clients. Clients with no 802.11w capability can also join.
<b>saquery-retry-time</b>	Time interval identified before which the SA query response is expected. If the controller does not get a response, another SA query is tried.
<i>saquery-retry-time-milliseconds</i>	The saquery retry time in milliseconds. The range is from 100 to 500 ms. The value must be specified in multiples of 100 milliseconds.

### Command Default

PMF is disabled.

### Command Modes

WLAN configuration

### Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

### Usage Guidelines

You must have WPA (Wi-Fi Protected Access) and AKM (Authentication Key Management) configured to use this feature. See Related Command section for more information on configuring the security parameters. 802.11w introduces an Integrity Group Temporal Key (IGTK) that is used to protect broadcast or multicast robust management frames. IGTK is a random value, assigned by the authenticator station (controller) used to protect MAC management protocol data units (MMPDUs) from the source STA. The 802.11w IGTK key is derived using the four-way handshake and is used only on WLANs that are configured with WPA2 security at Layer 2.

### Examples

This example shows how to enable the association comeback value at 15 seconds.

```
Controller(config-wlan)# security pmf association-comeback 15
```

This example shows how to configure mandatory 802.11w MPF protection for clients on a WLAN:

```
Controller(config-wlan)# security pmf mandatory
```

This example shows how to configure optional 802.11w MPF protection for clients on a WLAN:

```
Controller(config-wlan)# security pmf optional
```

This example shows how to configure the saquery parameter:

```
Controller(config-wlan)# security pmf saquery-retry-time 100
```

This example shows how to disable the PMF feature:

```
Controller(config-wlan)# no security pmf
```

### Related Commands

Command	Description
<a href="#">security wpa akm</a>	Configures authentication key-management using Cisco Centralized Key Management on a WLAN.

## security web-auth

To change the status of web authentication used on a WLAN, use the **security web-auth** command. To disable web authentication on a WLAN, use the **no** form of the command.

**security web-auth** [**authentication-list** *authentication-list-name*| **on-macfilter-failure**| **parameter-map** *parameter-map-name*]

**no security web-auth** [**authentication-list** [*authentication-list-name*]| **on-macfilter-failure**| **parameter-map** [*parameter-name*]]

### Syntax Description

<b>authentication-list</b> <i>authentication-list-name</i>	Sets the authentication list for IEEE 802.1x.
<b>on-macfilter-failure</b>	Enables web authentication on MAC failure.
<b>parameter-map</b> <i>parameter-map-name</i>	Configures the parameter map.

### Command Default

Web authentication is disabled.

### Command Modes

WLAN configuration

### Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

### Examples

The following example shows how to configure the authentication-list web authentication on a WLAN:

```
Controller(config-wlan) # security web-auth authentication-list test
```

## security wpa akm

To configure authentication key management using Cisco Centralized Key Management (CKKM), use the **security wpa akm** command. To disable the authentication key management for Cisco Centralized Key Management, use the **no** form of the command.

```
security wpa [akm {cckm|dot1x|ft|pmf|psk}|wpa1 [ciphers {aes|tkip}]] wpa2 [ciphers {aes|tkip}]]
no security wpa [akm {cckm|dot1x|ft|pmf|psk}|wpa1 [ciphers {aes|tkip}]] wpa2 [ciphers {aes|tkip}]]
```

### Syntax Description

<b>akm</b>	Configures the Authentication Key Management (AKM) parameters.
<b>aes</b>	Configures AES (Advanced Encryption Standard) encryption support.
<b>cckm</b>	Configures Cisco Centralized Key Management support.
<b>ciphers</b>	Configures WPA ciphers.
<b>dot1x</b>	Configures 802.1x support.
<b>ft</b>	Configures fast transition using 802.11r.
<b>pmf</b>	Configures 802.11w management frame protection.
<b>psk</b>	Configures 802.11r fast transition pre-shared key (PSK) support.
<b>tkip</b>	Configures Temporal Key Integrity Protocol (TKIP) encryption support.
<b>wpa2</b>	Configures Wi-Fi Protected Access 2 (WPA2) support.

### Command Default

By default Wi-Fi Protected Access2, 802.1x are enabled. WPA2, PSK, CCKM, FT dot1x, FT PSK, PMF dot1x, PMF PSK, FT Support are disabled. The FT Reassociation timeout is set to 20 seconds, PMF SA Query time is set to 200.

### Command Modes

WLAN configuration

**Command History**

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

**Examples**

The following example shows how to configure CCKM on the WLAN.

```
Controller(config-wlan)#security wpa akm cckm
```



## service-policy (WLAN)

To configure the WLAN quality of service (QoS) service policy, use the **service-policy** command. To disable a QoS policy on a WLAN, use the **no** form of this command.

**service-policy** [*client*] {*input*|*output*} *policy-name*

**no service-policy** [*client*] {*input*|*output*} *policy-name*

### Syntax Description

<b>client</b>	(Optional) Assigns a policy map to all clients in the WLAN.
<b>input</b>	Assigns an input policy map.
<b>output</b>	Assigns an output policy map.
<i>policy-name</i>	The policy name.

### Command Default

No policies are assigned and the state assigned to the policy is None.

### Command Modes

WLAN configuration

### Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

### Usage Guidelines

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

### Examples

This example shows how to configure the input QoS service policy on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# service-policy input policy-test
```

This example shows how to disable the input QoS service policy on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# no service-policy input policy-test
```

This example shows how to configure the output QoS service policy on a WLAN to platinum (precious metal policy):

```
Controller# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Controller(config)# wlan wlan1  
Controller(config-wlan)# service-policy output platinum
```

**Related Commands**

Command	Description
<a href="#">wlan</a>	Creates or disables a WLAN.
<a href="#">wlan</a>	Creates or disables a WLAN.

# session-timeout

To configure session timeout for clients associated to a WLAN, use the **session-timeout** command. To disable a session timeout for clients that are associated to a WLAN, use the **no** form of this command.

**session-timeout seconds**

**no session-timeout**

## Syntax Description

<i>seconds</i>	Timeout or session duration in seconds. A value of zero (0) is equivalent to no timeout. The range is from 300 to 86400.
----------------	--

## Command Default

The client timeout is set to 1800 seconds for WLANs that are configured with dot1x security. The client timeout is set to 0 for open WLANs.

## Command Modes

WLAN configuration

## Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

## Examples

This example shows how to configure a session timeout to 300 seconds:

```
Controller# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# session-timeout 300
```

This example shows how to disable a session timeout:

```
Controller# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# no session-timeout
```

# show wlan

To view WLAN parameters, use the **show wlan** command.

**show wlan** {**all** | **id** *wlan-id* | **name** *wlan-name* | **summary**}

## Syntax Description

<b>all</b>	Displays a summary of parameters of all configured WLANs. The list is ordered by the ascending order of the WLAN IDs.
<b>id</b> <i>wlan-id</i>	Specifies the wireless LAN identifier. The range is from 1 to 512.
<b>name</b> <i>wlan-name</i>	Specifies the WLAN profile name. The name is from 1 to 32 characters.
<b>summary</b>	Displays a summary of the parameters configured on a WLAN.

## Command Default

None

## Command Modes

Global configuration

## Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

## Examples

This example shows how to display a summary of the WLANs configured on the device:

```
Controller# show wlan summary
Number of WLANs: 1
```

WLAN Profile Name	SSID	VLAN Status
45 test-wlan	test-wlan-ssid	1 UP

This example shows how to display a summary of parameters configured on a particular WLAN:

```
Controller# show wlan name test-wlan
WLAN Identifier           : 45
Profile Name              : test-wlan
Network Name (SSID)      : test-wlan-ssid
Status                    : Enabled
Broadcast SSID            : Enabled
Maximum number of Associated Clients : 0
AAA Policy Override       : Disabled
Network Admission Control
  NAC-State                : Disabled
Number of Active Clients  : 0
Exclusionlist Timeout      : 60
```

```

Session Timeout                               : 1800 seconds
CHD per WLAN                                 : Enabled
Webauth DHCP exclusion                       : Disabled
Interface                                     : default
Interface Status                             : Up
Multicast Interface                          : test
WLAN IPv4 ACL                                : test
WLAN IPv6 ACL                                : unconfigured
DHCP Server                                  : Default
DHCP Address Assignment Required             : Disabled
DHCP Option 82                               : Disabled
DHCP Option 82 Format                        : ap-mac
DHCP Option 82 Ascii Mode                   : Disabled
DHCP Option 82 Rid Mode                     : Disabled
QoS Service Policy - Input
  Policy Name                                : unknown
  Policy State                               : None
QoS Service Policy - Output
  Policy Name                                : unknown
  Policy State                               : None
QoS Client Service Policy
  Input Policy Name                          : unknown
  Output Policy Name                         : unknown
WifiDirect                                   : Disabled
WMM                                           : Disabled
Channel Scan Defer Priority:
  Priority (default)                         : 4
  Priority (default)                         : 5
  Priority (default)                         : 6
Scan Defer Time (msecs)                     : 100
Media Stream Multicast-direct                : Disabled
CCX - AironetIe Support                     : Enabled
CCX - Gratuitous ProbeResponse (GPR)        : Disabled
CCX - Diagnostics Channel Capability         : Disabled
Dot11-Phone Mode (7920)                    : Invalid
Wired Protocol                              : None
Peer-to-Peer Blocking Action                 : Disabled
Radio Policy                                : All
DTIM period for 802.11a radio                : 1
DTIM period for 802.11b radio                : 1
Local EAP Authentication                    : Disabled
Mac Filter Authorization list name           : Disabled
Accounting list name                        : Disabled
802.1x authentication list name              : Disabled
Security
  802.11 Authentication                     : Open System
  Static WEP Keys                           : Disabled
  802.1X                                     : Disabled
  Wi-Fi Protected Access (WPA/WPA2)        : Enabled
    WPA (SSN IE)                           : Disabled
    WPA2 (RSN IE)                           : Enabled
    TKIP Cipher                             : Disabled
    AES Cipher                              : Enabled
    Auth Key Management                     :
      802.1x                               : Enabled
      PSK                                   : Disabled
      CCKM                                  : Disabled
  IP Security                               : Disabled
  IP Security Passthru                      : Disabled
  L2TP                                      : Disabled
  Web Based Authentication                  : Disabled
  Conditional Web Redirect                  : Disabled
  Splash-Page Web Redirect                  : Disabled
  Auto Anchor                              : Disabled
  Sticky Anchoring                         : Enabled
  Cranite Passthru                          : Disabled
  Fortress Passthru                        : Disabled
  PPTP                                      : Disabled
  Infrastructure MFP protection              : Enabled
  Client MFP                               : Optional
  Webauth On-mac-filter Failure             : Disabled
  Webauth Authentication List Name          : Disabled
  Webauth Parameter Map                    : Disabled

```

```
Tkip MIC Countermeasure Hold-down Timer : 60
Call Snooping                           : Disabled
Passive Client                           : Disabled
Non Cisco WGB                            : Disabled
Band Select                              : Disabled
Load Balancing                            : Disabled
IP Source Guard                           : Disabled
Netflow Monitor                           : test
      Direction                           : Input
      Traffic                             : Datalink

Mobility Anchor List
IP Address
-----
```

# shutdown

To disable a WLAN, use the **shutdown** command. To enable a WLAN, use the **no** form of this command.

**shutdown**

**no shutdown**

**Syntax Description** This command has no keywords or arguments.

**Command Default** None

**Command Modes** WLAN configuration

Command History	Release	Modification
	Cisco IOS XE 3.2SE	This command was introduced.

## Examples

This example shows how to disable a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Controller(config)# wlan test-wlan
Controller(config-wlan)# shutdown
Controller(config-wlan)# end
Controller# show wlan summary
Number of WLANs: 1
```

WLAN Profile Name	SSID	VLAN Status
45 test-wlan	test-wlan-ssid	1 DOWN

This example shows how to enable a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Controller(config)# wlan test-wlan
Controller(config-wlan)# no shutdown
Controller(config-wlan)# end
Controller# show wlan summary
Number of WLANs: 1
```

WLAN Profile Name	SSID	VLAN Status
45 test-wlan	test-wlan-ssid	1 UP

# sip-cac

To configure the Session Initiation Protocol (SIP) Call Admission Control (CAC) feature on a WLAN, use the **sip-cac** command. To disable the SIP CAC feature, use the **no** form of this command.

**sip-cac** {disassoc-client| send-486busy}

**no sip-cac** {disassoc-client| send-486busy}

## Syntax Description

<b>disassoc-client</b>	Enables a client disassociation if a CAC failure occurs.
<b>send-486busy</b>	Sends a SIP 486 busy message if a CAC failure occurs.

## Command Default

None

## Command Modes

WLAN configuration

## Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

## Usage Guidelines

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

## Examples

This example shows how to enable a client disassociation and 486 busy message on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# sip-cac disassoc-client
Controller(config-wlan)# sip-cac send-486busy
```

This example shows how to disable a client association and 486 busy message on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# no sip-cac disassoc-client
Controller(config-wlan)# no sip-cac send-486busy
```

## Related Commands

Command	Description
<a href="#">wlan</a>	Creates or disables a WLAN.



# static-ip tunneling

To enable static IP tunneling on a WLAN, use the **static-ip tunneling** command. To disable the static IP tunneling feature, use the **no** form of this command.

**static-ip tunneling**

**no static-ip tunneling**

**Syntax Description** This command has no keywords or arguments.

**Command Default** None

**Command Modes** WLAN configuration

Command History	Release	Modification
	Cisco IOS XE 3.2SE	This command was introduced.

## Examples

This example shows how to enable static-IP tunneling:

```
Controller# configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
Controller(config)# wlan wlan1  
Controller(config-wlan)# static-ip tunneling
```

This example shows how to disable static-IP tunneling:

```
Controller# configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
Controller(config)# wlan wlan1  
Controller(config-wlan)# no static-ip tunneling
```

# vlan

To assign a VLAN to an AP group, use the **vlan** command. To remove a VLAN ID, use the **no** form of this command.

**vlan** *interface-name*

**no vlan**

## Syntax Description

*interface-name*

VLAN interface name.

## Command Default

No VALN is assigned to the AP group. See Related Commands section for more information on how to disable a WLAN.

## Command Modes

WLAN AP Group configuration

## Command History

### Release

Cisco IOS XE 3.2SE

### Modification

This command was introduced.

## Usage Guidelines

You must disable the WLAN before using this command.

## Examples

This example shows how to configure a VLAN on an AP group:

```
Controller# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Controller(config)# ap group ap-group-1
Controller(config-apgroup)# wlan test-wlan
Controller(config-wlan-apgroup)# vlan 3
```

## Related Commands

### Command

[wlan](#)

### Description

Creates or disables a WLAN.

## wgb non-cisco

To enable non-Cisco Workgroup Bridges (WGB) clients on the WLAN, use the **wgb non-cisco** command. To disable support for non-Cisco WGB clients, use the **no** form of this command.

**wgb non-cisco**

**no wgb non-cisco**

**Syntax Description** This command has no keywords or arguments.

**Command Default** Non-Cisco WGB clients are disabled.

**Command Modes** WLAN configuration

Command History	Release	Modification
	Cisco IOS XE 3.2SE	This command was introduced.

**Usage Guidelines** You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

**Examples** This example shows how to enable non-Cisco WGBs on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# shutdown
Controller(config-wlan)# wgb non-cisco
Controller(config-wlan)# no shutdown
```

This example shows how to disable support for non-Cisco WGB clients on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# shutdown
Controller(config-wlan)# no wgb non-cisco
Controller(config-wlan)# no shutdown
```

# wifidirect policy

To configure Wi-Fi Direct client policy on a WLAN, use the **wifidirect policy** command. To disable Wi-Fi Direct Client policy, use the **no** form of the command.

**wifidirect policy {permit| deny}**

## Syntax Description

<b>permit</b>	Enables Wi-Fi Direct clients to associate with the WLAN.
<b>deny</b>	<p>When the Wi-Fi Direct policy is configured as "deny", the controller permits or denies Wi-Fi Direct devices based on the device capabilities. A Wi-Fi Direct device reports these capabilities in its association request to the controller and these are based on the Wi-Fi capabilities of the device. These include:</p> <ul style="list-style-type: none"> <li>• Concurrent Operation</li> <li>• Cross connection</li> </ul> <p>If the Wi-Fi device supports either concurrent operations or cross connections or both, the client association is denied. The client can associate if the device does not support concurrent operations and cross connections.</p>

## Command Default

Wi-Fi Direct is disabled.

## Command Modes

WLAN configuration

## Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

## Examples

The following example shows how to enable Wi-Fi Direct and configure the Wi-Fi Direct clients to associate with the WLAN:

```
Controller(config-wlan) # wifidirect policy permit
```

## wlan (AP Group Configuration)

To configure WLAN parameters of a WLAN in an access point (AP) group, use the **wlan** command. To remove a WLAN from the AP group, use the **no** form of this command.

**wlan** *wlan-name*

**no wlan** *wlan-name*

### Syntax Description

<i>wlan-name</i>	WLAN profile name. The range is from 1 to 32 alphanumeric characters.
------------------	---

### Command Default

WLAN parameters are not configured for an AP group.

### Command Modes

AP Group configuration

### Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

### Usage Guidelines

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

### Examples

This example shows how to configure WLAN related parameters in the AP group configuration mode:

```
Controller# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Controller(config)# ap group test
Controller(config-apgroup)# wlan qos-wlan
```

### Related Commands

Command	Description
<a href="#">wlan</a>	Creates or disables a WLAN.

# wlan

To create a wireless LAN, use the **wlan** command. To disable a wireless LAN, use the **no** form of this command.

**wlan** [*wlan-name*| *wlan-name wlan-id*| *wlan-name wlan-id wlan-ssid*]

**no wlan** [*wlan-name*| *wlan-name wlan-id*| *wlan-name wlan-id wlan-ssid*]

## Syntax Description

<i>wlan-name</i>	WLAN profile name. The name is from 1 to 32 alphanumeric characters.
<i>wlan-id</i>	Wireless LAN identifier. The range is from 1 to 512.
<i>wlan-ssid</i>	SSID. The range is from 1 to 32 alphanumeric characters.

## Command Default

WLAN is disabled.

## Command Modes

Global configuration

## Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

## Usage Guidelines

If you do not specify an SSID, the profile name parameter is used for both the profile name and the SSID. If the management and AP-manager interfaces are mapped to the same port and are members of the same VLAN, you must disable the WLAN before making a port-mapping change to either interface. If the management and AP-manager (Access Point Manager) interfaces are assigned to different VLANs, you do not need to disable the WLAN.

An error message appears if you try to delete a WLAN that is assigned to an access point group. If you proceed, the WLAN is removed from the access point group and from the access point's radio.

## Examples

This example shows how to create a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config)# wlan test-wlan-cr 67 test-wlan-cr-ssid
```

This example shows how to delete a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config)# no wlan test-wlan-cr 67 test-wlan-cr-ssid
```

# wlan shutdown

To disable a WLAN, use the **wlan shutdown** command. To enable a WLAN, use the **no** form of this command.

**wlan shutdown**

**no wlan shutdown**

**Command Default** The WLAN is disabled.

**Command Modes** Global configuration

Command History	Release	Modification
	Cisco IOS XE 3.2SE	This command was introduced.

**Usage Guidelines** You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

**Examples** This example shows how to shut down a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# shutdown
```

Related Commands	Command	Description
	<a href="#">wlan</a>	Creates or disables a WLAN.

## wmm

To enable Wi-Fi Multimedia (WMM) on a WLAN, use the **wmm** command. To disable WMM on a WLAN, use the **no** form of this command.

**wmm {allowed| require}**

**no wmm**

### Syntax Description

<b>allowed</b>	Allows WMM on a WLAN.
<b>require</b>	Mandates that clients use WMM on the WLAN.

### Command Default

WMM is enabled.

### Command Modes

WLAN configuration

### Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

### Usage Guidelines

When the controller is in Layer 2 mode and WMM is enabled, you must put the access points on a trunk port in order to allow them to join the controller.

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

### Examples

This example shows how to enable WMM on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# wmm allowed
```

This example shows how to disable WMM on a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config-wlan)# no wmm
```

### Related Commands

Command	Description
<a href="#">wlan</a>	Creates or disables a WLAN.