Config Commands: r to z

config radius acct

To configure settings for a RADIUS accounting server for the Cisco wireless LAN controller, use the **config radius acct** command.

config radius acct { {**add** *index IP addr port* {**ascii** | **hex**} *secret*} | **delete** *index* | **disable** *index* | **enable** *index* | **ipsec** {**authentication** {**hmac-md5** *index* | **hmac-sha1** *index* } | **disable** *index* | **enable** *index* | **encryption** {**256-aes** | **3des** | **aes** | **des**} *index* | **ike** {**auth-mode** {**pre-shared-key** *index type shared_secret_key* | **certificate** *index* } | **dh-group** { **2048bit-group-14** | **group-1** | **group-2** | **group-5**} *index* | **lifetime** *seconds index* | **phase1** {**aggressive** | **main**} *index* } } | {**mac-delimiter** {**colon** | **hyphen** | **none** | **single-hyphen**}} | {**network** *index* {**disable** | **enable**}} | {**region** {**group** | **none** | **provincial**}} | **retransmit-timeout** *index seconds* | **realm** {**add** | **delete**} *index realm-string*}

Syntax Description

add	Adds a RADIUS accounting server (IPv4 or IPv6).
index	RADIUS server index (1 to 17).
IP addr	RADIUS server IP address (IPv4 or IPv6).
port	RADIUS server's UDP port number for the interface protocols.
ascii	Specifies the RADIUS server's secret type: **ascii**.
hex	Specifies the RADIUS server's secret type: **hex**.
secret	RADIUS server's secret.
enable	Enables a RADIUS accounting server.
disable	Disables a RADIUS accounting server.
delete	Deletes a RADIUS accounting server.
ipsec	Enables or disables IPSec support for an accounting server. **Note** IPSec is not supported for IPv6.
authentication	Configures IPSec Authentication.
hmac-md5	Enables IPSec HMAC-MD5 authentication.
hmac-sha1	Enables IPSec HMAC-SHA1 authentication.
disable	Disables IPSec support for an accounting server.
enable	Enables IPSec support for an accounting server.
encryption	Configures IPSec encryption.
256-aes	Enables IPSec AES-256 encryption.

3des	Enables IPSec 3DES encryption.
aes	Enables IPSec AES-128 encryption.
des	Enables IPSec DES encryption.
ike	Configures Internet Key Exchange (IKE).
auth-mode	Configures IKE authentication method.
pre-shared-key	Pre-shared key for authentication.
certificate	Certificate used for authentication.
dh-group	Configures IKE Diffie-Hellman group.
2048bit-group-14	Configures DH group 14 (2048 bits).
group-1	Configures DH group 1 (768 bits).
group-2	Configures DH group 2 (1024 bits).
group-5	Configures DH group 5 (1536 bits).
lifetime *seconds*	Configures IKE lifetime in seconds. The range is from 1800 to 57600 seconds and the default is 28800.
phase1	Configures IKE phase1 mode.
aggressive	Enables IKE aggressive mode.
main	Enables IKE main mode.
mac-delimiter	Configures MAC delimiter for caller station ID and calling station ID.
colon	Sets the delimiter to colon (For example: xx:xx:xx:xx:xx:xx).
hyphen	Sets the delimiter to hyphen (For example: xx-xx-xx-xx-xx-xx).
none	Disables delimiters (For example: xxxxxxxxxx).
single-hyphen	Sets the delimiters to single hyphen (For example: xxxxxx-xxxxxx).
network	Configures a default RADIUS server for network users.
group	Specifies RADIUS server type group.
none	Specifies RADIUS server type none.
provincial	Specifies RADIUS server type provincial.

retransmit-timeout	Changes the default retransmit timeout for the server.
seconds	The number of seconds between retransmissions.
realm	Specifies radius acct realm.
add	Adds radius acct realm.
delete	Deletes radius acct realm.

Command Default

When adding a RADIUS server, the port number defaults to 1813 and the state is **enabled**.

Usage Guidelines

IPSec is not supported for IPv6.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports both IPv4 and IPv6 address formats.

The following example shows how to configure a priority 1 RADIUS accounting server at *10.10.10.10* using port *1813* with a login password of *admin*:

```
(Cisco Controller) > config radius acct add 1 10.10.10.10 1813 ascii admin
```

The following example shows how to configure a priority 1 RADIUS accounting server at *2001:9:6:40::623* using port *1813* with a login password of *admin*:

```
(Cisco Controller) > config radius acct add 1 2001:9:6:40::623 1813 ascii admin
```

config radius acct ipsec authentication

To configure IPsec authentication for the Cisco wireless LAN controller, use the **config radius acct ipsec authentication** command.

config radius acct ipsec authentication {**hmac-md5** | **hmac-sha1**} *index*

Syntax Description

hmac-md5	Enables IPsec HMAC-MD5 authentication.
hmac-sha1	Enables IPsec HMAC-SHA1 authentication.
index	RADIUS server index.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the IPsec hmac-md5 authentication service on the RADIUS accounting server index 1:

```
(Cisco Controller) > config radius acct ipsec authentication hmac-md5 1
```

Related Commands

show radius acct statistics

config radius acct ipsec disable

To disable IPsec support for an accounting server for the Cisco wireless LAN controller, use the **config radius acct ipsec disable** command.

config radius acct ipsec disable *index*

Syntax Description

index	RADIUS server index.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to disable the IPsec support for RADIUS accounting server index 1:

```
(Cisco Controller) > config radius acct ipsec disable 1
```

Related Commands

show radius acct statistics

config radius acct ipsec enable

To enable IPsec support for an accounting server for the Cisco wireless LAN controller, use the **config radius acct ipsec enable** command.

config radius acct ipsec enable *index*

Syntax Description

index	RADIUS server index.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Examples

The following example shows how to enable the IPsec support for RADIUS accounting server index 1:

```
(Cisco Controller) > config radius acct ipsec enable 1
```

Related Commands

show radius acct statistics

config radius acct ipsec encryption

To configure IPsec encryption for an accounting server for the Cisco wireless LAN controller, use the **config radius acct ipsec encryption** command.

config radius acct ipsec encryption {**3des** | **aes** | **des**} *index*

Syntax Description

256-aes	Enables IPSec AES-256 encryption.
3des	Enables IPsec 3DES encryption.
aes	Enables IPsec AES encryption.
des	Enables IPsec DES encryption.
index	RADIUS server index value of between 1 and 17.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the IPsec 3DES encryption for RADIUS server index value 3:

```
(Cisco Controller) > config radius acct ipsec encryption 3des 3
```

config radius acct ipsec ike

To configure Internet Key Exchange (IKE) for the Cisco WLC, use the **config radius acct ipsec ike** command.

config radius acct ipsec ike dh-group {**group-1** | **group-2** | **group-5** | **group-14**} | **lifetime** *seconds* | **phase1** {**aggressive** | **main**}} *index*

Syntax Description

dh-group	Specifies the Dixie-Hellman (DH) group.
group-1	Configures the DH Group 1 (768 bits).
group-2	Configures the DH Group 2 (1024 bits).
group-5	Configures the DH Group 5 (1024 bits).
group-5	Configures the DH Group 14 (2048 bits).
lifetime	Configures the IKE lifetime.
seconds	IKE lifetime in seconds.
phase1	Configures the IKE phase1 node.
aggressive	Enables the aggressive mode.
main	Enables the main mode.
index	RADIUS server index.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure an IKE lifetime of 23 seconds for RADIUS server index 1:

```
(Cisco Controller) > config radius acct ipsec ike lifetime 23 1
```

Related Commands

show radius acct statistics

config radius acct mac-delimiter

To specify the delimiter to be used in the MAC addresses that are sent to the RADIUS accounting server, use the **config radius acct mac-delimiter** command.

config radius acct mac-delimiter {**colon** | **hyphen** | **single-hyphen** | **none**}

Syntax Description

colon	Sets the delimiter to a colon (for example, xx:xx:xx:xx:xx:xx).
hyphen	Sets the delimiter to a hyphen (for example, xx-xx-xx-xx-xx-xx).
single-hyphen	Sets the delimiter to a single hyphen (for example, xxxxxx-xxxxxx).
none	Disables the delimiter (for example, xxxxxxxxxxxx).

Command Default

The default delimiter is a hyphen.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to set the delimiter hyphen to be used in the MAC addresses that are sent to the RADIUS accounting server for the network users:

```
(Cisco Controller) > config radius acct mac-delimiter hyphen
```

Related Commands

show radius acct statistics

config radius acct network

To configure a default RADIUS server for network users, use the **config radius acct network** command.

config radius acct network *index* {**enable** | **disable**}

Syntax Description

index	RADIUS server index.
enable	Enables the server as a network user's default RADIUS server.
disable	Disables the server as a network user's default RADIUS server.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure a default RADIUS accounting server for the network users with RADIUS server index1:

```
(Cisco Controller) > config radius acct network 1 enable
```

Related Commands

show radius acct statistics

config radius acct realm

To configure realm on RADIUS accounting server, use the **config radius acct realm** command.

config radius acct realm {**add** | **delete**} *radius_index realm_string*

Syntax Description

radius_server	Radius server index. The range is from 1 to 17.
add	Add realm to RADIUS accounting server.
delete	Delete realm from RADIUS accounting server.
realm_string	Unique string associated to RADIUS accounting realm.

Command Default

None

Command History

Release	Modification
8.0	This command was introduced.

The following example shows how add realm to the RADIUS accounting server:

```
(Cisco Controller) > config radius acct realm add 3 test
```

config radius acct retransmit-timeout

To change the default transmission timeout for a RADIUS accounting server for the Cisco wireless LAN controller, use the **config radius acct retransmit-timeout** command.

config radius acct retransmit-timeout *index timeout*

Syntax Description

index	RADIUS server index.
timeout	Number of seconds (from 2 to 30) between retransmissions.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure retransmission timeout value 5 seconds between the retransmission:

```
(Cisco Controller) > config radius acct retransmit-timeout 5
```

Related Commands

show radius acct statistics

config radius auth

To configure settings for a RADIUS authentication server for the Cisco wireless LAN controller, use the **config radius auth** command.

config radius auth {**add** *index IP addr portascii/hexsecret*} | | **delete** *index* | **disable** *index* | **enable** *index* | **framed-mtu** *mtu* | { **ipsec** {**authentication** {**hmac-md5** *index* | **hmac-sha1** *index* } | **disable** *index* | **enable** *index* | **encryption** {**256-aes** | **3des** | **aes** | **des**} *index* | **ike** {**auth-mode** {**pre-shared-key** *index ascii/hex shared_secret* | **certificate** *index* } | **dh-group** { **2048bit-group-14** | **group-1** | **group-2** | **group-5**} *index* | **lifetime** *seconds index* | **phase1** {**aggressive** | **main**} *index* } } | { { **keywrap**{**add** *ascii/hex kek mack index* } | **delete** *index* | **disable** | **enable**} } | {**mac-delimiter** {**colon** | **hyphen** | **none** | **single-hyphen**}} | {{**management** *index* {**enable** | **disable**}} | { **mgmt-retransmit-timeout** *index Retransmit Timeout* } | { **network** *index* {**enable** | **disable**}} | {**realm** {**add** | **delete**} *radius-index realm-string*} } | {**region** {**group** | **none** | **provincial**}} | {**retransmit-timeout** *index Retransmit Timeout*} | { **rfc3576** {**enable** | **disable**} *index* }

Syntax Description

enable	Enables a RADIUS authentication server.
disable	Disables a RADIUS authentication server.
delete	Deletes a RADIUS authentication server.
index	RADIUS server index. The controller begins the search with 1. The server index range is from 1 to 17.
add	Adds a RADIUS authentication server. See the “Defaults” section.
IP addr	IP address (IPv4 or IPv6) of the RADIUS server.
port	RADIUS server’s UDP port number for the interface protocols.
ascii/hex	Specifies RADIUS server’s secret type: **ascii** or **hex**.
secret	RADIUS server’s secret.
callStationIdType	Configures Called Station Id information sent in RADIUS authentication messages.
framed-mtu	Configures the Framed-MTU for all the RADIUS servers. The framed-mtu range is from 64 to 1300 bytes.
ipsec	Enables or disables IPSEC support for an authentication server. **Note** IPSec is not supported for IPv6.
keywrap	Configures RADIUS keywrap.

ascii/hex	Specifies the input format of the keywrap keys.
kek	Enters the 16-byte key-encryption-key.
mack	Enters the 20-byte message-authenticator-code-key.
mac-delimiter	Configures MAC delimiter for caller station ID and calling station ID.
management	Configures a RADIUS Server for management users.
mgmt-retransmit-timeout	Changes the default management login retransmission timeout for the server.
network	Configures a default RADIUS server for network users.
realm	Configures radius auth realm.
region	Configures RADIUS region property.
retransmit-timeout	Changes the default network login retransmission timeout for the server.
rfc3576	Enables or disables RFC-3576 support for an authentication server.

Command Default

When adding a RADIUS server, the port number defaults to 1812 and the state is **enabled**.

Usage Guidelines

IPSec is not supported for IPv6.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports both IPv4 and IPv6 address formats.

The following example shows how to configure a priority *3* RADIUS authentication server at *10.10.10.10* using port *1812* with a login password of *admin*:

```
(Cisco Controller) > config radius auth add 3 10.10.10.10 1812 ascii admin
```

The following example shows how to configure a priority *3* RADIUS authentication server at *2001:9:6:40::623* using port *1812* with a login password of *admin*:

```
(Cisco Controller) > config radius auth add 3 2001:9:6:40::623 1812 ascii admin
```

config radius auth callStationIdType

To configure the RADIUS authentication server, use the **config radius auth callStationIdType** command.

config radius auth callStationIdType {**ap-ethmac-only** | **ap-ethmac-ssid** | **ap-group-name** | **ap-label-address** | **ap-label-address-ssid** | **ap-location** | **ap-mac-ssid-ap-group** | **ap-macaddr-only** | **ap-macaddr-ssid** | **ap-name** | **ap-name-ssid** | **flex-group-name** | **ipaddr** | **macaddr** | **vlan-id**}

Syntax Description

ipaddr	Configures the Call Station ID type to use the IP address (only Layer 3).
macaddr	Configures the Call Station ID type to use the system's MAC address (Layers 2 and 3).
ap-macaddr-only	Configures the Call Station ID type to use the access point's MAC address (Layers 2 and 3).
ap-macaddr-ssid	Configures the Call Station ID type to use the access point's MAC address (Layers 2 and 3) in the format *AP MAC address*:*SSID*.
ap-ethmac-only	Configures the Called Station ID type to use the access point's Ethernet MAC address.
ap-ethmac-ssid	Configures the Called Station ID type to use the access point's Ethernet MAC address in the format *AP Ethernet MAC address*:*SSID*.
ap-group-name	Configures the Call Station ID type to use the AP group name. If the AP is not part of any AP group, default-group is taken as the AP group name.
flex-group-name	Configures the Call Station ID type to use the FlexConnect group name. If the FlexConnect AP is not part of any FlexConnect group, the system MAC address is taken as the Call Station ID.
ap-name	Configures the Call Station ID type to use the access point's name.
ap-name-ssid	Configures the Call Station ID type to use the access point's name in the format *AP name*:*SSID*
ap-location	Configures the Call Station ID type to use the access point's location.
ap-mac-ssid-ap-group	Sets Called Station ID type to the format <AP MAC address>:<SSID>:<AP Group>
vlan-id	Configures the Call Station ID type to use the system's VLAN-ID.

ap-label-address	Configures the Call Station ID type to the AP MAC address that is printed on the AP label, for the accounting messages.
ap-label-address-ssid	Configures the Call Station ID type to the AP MAC address:SSID format.

Command Default

The MAC address of the system.

Usage Guidelines

The controller sends the Called Station ID attribute to the RADIUS server in all authentication and accounting packets. The Called Station ID attribute can be used to classify users to different groups based on the attribute value. The command is applicable only for the Called Station and not for the Calling Station.

You cannot send only the SSID as the Called-Station-ID, you can only combine the SSID with either the access point MAC address or the access point name.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
7.6	The **ap-ethmac-only** and **ap-ethmac-ssid** keywords were added to support the access point's Ethernet MAC address. The **ap-label-address** and **ap-label-address-ssid** keywords were added.
8.0	This command supports both IPv4 and IPv6 address formats.
8.3	The **ap-mac-ssid-ap-group** keyword was added.

The following example shows how to configure the call station ID type to use the IP address:

```
(Cisco Controller) > config radius auth callStationIdType ipAddr
```

The following example shows how to configure the call station ID type to use the system's MAC address:

```
(Cisco Controller) > config radius auth callStationIdType macAddr
```

The following example shows how to configure the call station ID type to use the access point's MAC address:

```
(Cisco Controller) > config radius auth callStationIdType ap-macAddr
```

config radius auth framed-mtu

To configure the framed-mtu value for all RADIUS servers, use the **config radius auth framed-mtu** command.

config radius auth framed-mtu *mtu*

Syntax Description

mtu	Framed-MTU value range between 64 and 1300 bytes **Note** Controller does not use or fragment the framed MTU in the controller. This AV pair that is configurable on the controller is part of the authentication request packet to the RADIUS server and is used to allow the RADIUS server to fragment large packets during events such as 802.1x exchange.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced.

The following example shows how to set the framed-mtu value for a RADIUS authentication server:

```
(Cisco Controller) > config radius auth framed-mtu 500
```

config radius auth IPsec authentication

To configure IPsec support for an authentication server for the Cisco wireless LAN controller, use the **config radius auth IPsec authentication** command.

config radius auth IPsec authentication {**hmac-md5** | **hmac-sha1**} *index*

Syntax Description

hmac-md5	Enables IPsec HMAC-MD5 authentication.
hmac-shal	Enables IPsec HMAC-SHA1 authentication.
index	RADIUS server index.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the IPsec hmac-md5 support for RADIUS authentication server index 1:

```
(Cisco Controller) > config radius auth IPsec authentication hmac-md5 1
```

Related Commands

show radius acct statistics

config radius auth ipsec disable

To disable IPsec support for an authentication server for the Cisco wireless LAN controller, use the **config radius auth IPsec disable** command.

config radius auth ipsec {**enable** | **disable**} *index*

Syntax Description

enable	Enables the IPsec support for an authentication server.
disable	Disables the IPsec support for an authentication server.
index	RADIUS server index.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

This example shows how to enable the IPsec support for RADIUS authentication server index 1:

```
(Cisco Controller) > config radius auth ipsec enable 1
```

This example shows how to disable the IPsec support for RADIUS authentication server index 1:

```
(Cisco Controller) > config radius auth ipsec disable 1
```

Related Commands

show radius acct statistics

config radius auth ipsec encryption

To configure IPsec encryption support for an authentication server for the Cisco wireless LAN controller, use the **config radius auth ipsec encryption** command.

config radius auth IPsec encryption {**256-aes** | **3des** | **aes** | **des**} *index*

Syntax Description

256-aes	Enables the IPsec 256 AES encryption.
3des	Enables the IPsec 3DES encryption.
aes	Enables the IPsec AES encryption.
des	Enables the IPsec DES encryption.
index	RADIUS server index.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	The keyword 256-aes was added.

The following example shows how to configure IPsec 3dec encryption RADIUS authentication server index 3:

```
(Cisco Controller) > config radius auth ipsec encryption 3des 3
```

Related Commands

show radius acct statistics

config radius auth ipsec ike

To configure Internet Key Exchange (IKE) for the Cisco wireless LAN controller, use the **config radius auth IPsec ike** command.

config radius auth ipsec ike {**auth-mode** {**pre-shared-key***index* {**ascii** | **hex** *shared-secret*} | **certificate** *index* } **dh-group** {**2048bit-group-14** | **group-1** | **group-2** | **group-5**} | **lifetime** *seconds* | **phase1** {**aggressive** | **main**}} *index*

Syntax Description

auth-mode	Configures the IKE authentication method.
pre-shared-key	Configures the preshared key for IKE authentication method.
index	RADIUS server index between 1 and 17.
ascii	Configures RADIUS IPsec IKE secret in an ASCII format.
hex	Configures RADIUS IPsec IKE secret in a hexadecimal format.
shared-secret	Configures the shared RADIUS IPsec secret.
certificate	Configures the certificate for IKE authentication.
dh-group	Configures the IKE Diffe-Hellman group.
2048bit-group-14	Configures the DH Group14 (2048 bits).
group-1	Configures the DH Group 1 (768 bits).
group-2	Configures the DH Group 2 (1024 bits).
group-5	Configures the DH Group 2 (1024 bits).
lifetime	Configures the IKE lifetime.
seconds	IKE lifetime in seconds. The range is from 1800 to 57600 seconds.
phase1	Configures the IKE phase1 mode.
aggressive	Enables the aggressive mode.
main	Enables the main mode.
index	RADIUS server index.

Command Default

By default, preshared key is used for IPsec sessions and IKE lifetime is 28800 seconds.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure IKE lifetime of 23 seconds for RADIUS authentication server index 1:

```
(Cisco Controller) > config radius auth ipsec ike lifetime 23 1
```

Related Commands

show radius acct statistics

config radius auth keywrap

To enable and configure Advanced Encryption Standard (AES) key wrap, which makes the shared secret between the controller and the RADIUS server more secure, use the **config radius auth keywrap** command.

config radius auth keywrap {**enable** | **disable** | **add** {**ascii** | **hex**} *kek mack* | **delete**} *index*

Syntax Description

enable	Enables AES key wrap.
disable	Disables AES key wrap.
add	Configures AES key wrap attributes.
ascii	Configures key wrap in an ASCII format.
hex	Configures key wrap in a hexadecimal format.
kek	16-byte Key Encryption Key (KEK).
mack	20-byte Message Authentication Code Key (MACK).
delete	Deletes AES key wrap attributes.
index	Index of the RADIUS authentication server on which to configure the AES key wrap.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the AES key wrap for a RADIUS authentication server:

```
(Cisco Controller) > config radius auth keywrap enable
```

Related Commands

show radius auth statistics

config radius auth mac-delimiter

To specify a delimiter to be used in the MAC addresses that are sent to the RADIUS authentication server, use the **config radius auth mac-delimiter** command.

config radius auth mac-delimiter {**colon** | **hyphen** | **single-hyphen** | **none**}

Syntax Description

colon	Sets a delimiter to a colon (for example, xx:xx:xx:xx:xx:xx).
hyphen	Sets a delimiter to a hyphen (for example, xx-xx-xx-xx-xx-xx).
single-hyphen	Sets a delimiter to a single hyphen (for example, xxxxxx-xxxxxx).
none	Disables the delimiter (for example, xxxxxxxxxxxx).

Command Default

The default delimiter is a hyphen.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to specify a delimiter hyphen to be used for a RADIUS authentication server:

```
(Cisco Controller) > config radius auth mac-delimiter hyphen
```

Related Commands

show radius auth statistics

config radius auth management

To configure a default RADIUS server for management users, use the **config radius auth management** command.

config radius auth management *index* {**enable** | **disable**}

Syntax Description

index	RADIUS server index.
enable	Enables the server as a management user's default RADIUS server.
disable	Disables the server as a management user's default RADIUS server.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure a RADIUS server for management users:

```
(Cisco Controller) > config radius auth management 1 enable
```

Related Commands

show radius acct statistics

config radius acct network

config radius auth mgmt-retransmit-timeout

config radius auth mgmt-retransmit-timeout

To configure a default RADIUS server retransmission timeout for management users, use the **config radius auth mgmt-retransmit-timeout** command.

config radius auth mgmt-retransmit-timeout *index retransmit-timeout*

Syntax Description

index	RADIUS server index.
retransmit-timeout	Timeout value. The range is from 1 to 30 seconds.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure a default RADIUS server retransmission timeout for management users:

```
(Cisco Controller) > config radius auth mgmt-retransmit-timeout 1 10
```

Related Commands

config radius auth management

config radius auth network

To configure a default RADIUS server for network users, use the **config radius auth network** command.

config radius auth network *index* {**enable** | **disable**}

Syntax Description

index	RADIUS server index.
enable	Enables the server as a network user default RADIUS server.
disable	Disables the server as a network user default RADIUS server.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure a default RADIUS server for network users:

```
(Cisco Controller) > config radius auth network 1 enable
```

Related Commands

show radius acct statistics

config radius acct network

config radius auth realm

To configure realm on RADIUS authentication server, use the **config radius auth realm** command.

config radius auth realm {**add** | **delete**} *radius_index realm_string*

Syntax Description

radius_server	Radius server index. The range is from 1 to 17.
add	Add realm to RADIUS authentication server.
delete	Delete realm from RADIUS authentication server.
realm_string	Unique string associated to RADIUS authentication realm.

Command Default

None

Command History

Release	Modification
8.0	This command was introduced.

The following example shows how add realm to the RADIUS authentication server:

```
(Cisco Controller) > config radius auth realm add 3 test
```

config radius auth retransmit-timeout

To change a default transmission timeout for a RADIUS authentication server for the Cisco wireless LAN controller, use the **config radius auth retransmit-timeout** command.

config radius auth retransmit-timeout *index timeout*

Syntax Description

index	RADIUS server index.
timeout	Number of seconds (from 2 to 30) between retransmissions.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure a retransmission timeout of 5 seconds for a RADIUS authentication server:

```
(Cisco Controller) > config radius auth retransmit-timeout 5
```

Related Commands

show radius auth statistics

config radius auth rfc3576

To configure RADIUS RFC-3576 support for the authentication server for the Cisco WLC, use the **config radius auth rfc3576** command.

config radius auth rfc3576 {**enable** | **disable**} *index*

Syntax Description

enable	Enables RFC-3576 support for an authentication server.
disable	Disables RFC-3576 support for an authentication server.
index	RADIUS server index.

Command Default

Disabled

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

RFC 3576, which is an extension to the RADIUS protocol, allows dynamic changes to a user session. RFC 3576 includes support for disconnecting users and changing authorizations applicable to a user session. Disconnect messages cause a user session to be terminated immediately; CoA messages modify session authorization attributes such as data filters.

The following example shows how to enable the RADIUS RFC-3576 support for a RADIUS authentication server:

```
(Cisco Controller) > config radius auth rfc3576 enable 2
```

Related Commands

show radius auth statistics

show radius summary

show radius rfc3576

config radius auth retransmit-timeout

To configure a retransmission timeout value for a RADIUS accounting server, use the **config radius auth server-timeout** command.

config radius auth retransmit-timeout *index timeout*

Syntax Description

index	RADIUS server index.
timeout	Timeout value. The range is from 2 to 30 seconds.

Command Default

The default timeout is 2 seconds.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure a server timeout value of 2 seconds for RADIUS authentication server index 10:

```
(Cisco Controller) > config radius auth retransmit-timeout 2 10
```

Related Commands

show radius auth statistics

show radius summary

config radius aggressive-failover disabled

To configure the controller to mark a RADIUS server as down (not responding) after the server does not reply to three consecutive clients, use the **config radius aggressive-failover disabled** command.

config radius aggressive-failover disabled

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the controller to mark a RADIUS server as down:

```
(Cisco Controller) > config radius aggressive-failover disabled
```

Related Commands

show radius summary

config radius backward compatibility

To configure RADIUS backward compatibility for the Cisco wireless LAN controller, use the **config radius backward compatibility** command.

config radius backward compatibility {**enable** | **disable**}

Syntax Description

enable	Enables RADIUS vendor ID backward compatibility.
disable	Disables RADIUS vendor ID backward compatibility.

Command Default

Enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the RADIUS backward compatibility settings:

```
(Cisco Controller) > config radius backward compatibility disable
```

Related Commands

show radius summary

config radius callStationIdCase

To configure callStationIdCase information sent in RADIUS messages for the Cisco WLC, use the **config radius callStationIdCase** command.

config radius callStationIdCase {**legacy** | **lower** | **upper**}

Syntax Description

legacy	Configures Call Station IDs for Layer 2 authentication to RADIUS in uppercase.
lower	Configures all Call Station IDs to RADIUS in lowercase.
upper	Configures all Call Station IDs to RADIUS in uppercase.

Command Default

Enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to send the call station ID in lowercase:

```
(Cisco Controller) > config radius callStationIdCase lower
```

Related Commands

show radius summary

config radius callStationIdType

To configure the Called Station ID type information sent in RADIUS accounting messages for the Cisco wireless LAN controller, use the **config radius callStationIdType** command.

config radius callStationIdType {**ap-ethmac-only** | **ap-ethmac-ssid** | **ap-group-name** | **ap-label-address** | **ap-label-address-ssid** | **ap-location** | **ap-mac-ssid-ap-group** | **ap-macaddr-only** | **ap-macaddr-ssid** | **ap-name** | **ap-name-ssid** | **flex-group-name** | **ipaddr** | **macaddr** | **vlan-id**}

Syntax Description

ipaddr	Configures the Call Station ID type to use the IP address (only Layer 3).
macaddr	Configures the Call Station ID type to use the system's MAC address (Layers 2 and 3).
ap-macaddr-only	Configures the Call Station ID type to use the access point's MAC address (Layers 2 and 3).
ap-macaddr-ssid	Configures the Call Station ID type to use the access point's MAC address (Layers 2 and 3) in the format *AP MAC address*:*SSID*.
ap-ethmac-only	Configures the Called Station ID type to use the access point's Ethernet MAC address.
ap-ethmac-ssid	Configures the Called Station ID type to use the access point's Ethernet MAC address in the format *AP Ethernet MAC address*:*SSID*.
ap-group-name	Configures the Call Station ID type to use the AP group name. If the AP is not part of any AP group, default-group is taken as the AP group name.
flex-group-name	Configures the Call Station ID type to use the FlexConnect group name. If the FlexConnect AP is not part of any FlexConnect group, the system MAC address is taken as the Call Station ID.
ap-name	Configures the Call Station ID type to use the access point's name.
ap-name-ssid	Configures the Call Station ID type to use the access point's name in the format *AP name*:*SSID*
ap-location	Configures the Call Station ID type to use the access point's location.
ap-mac-ssid-ap-group	Sets Called Station ID type to the format <AP MAC address>:<SSID>:<AP Group>
vlan-id	Configures the Call Station ID type to use the system's VLAN-ID.

ap-label-address	Configures the Call Station ID type to the AP MAC address that is printed on the AP label, for the accounting messages.
ap-label-address-ssid	Configures the Call Station ID type to the AP MAC address:SSID format.

Command Default

The IP address of the system.

Usage Guidelines

The controller sends the Called Station ID attribute to the RADIUS server in all authentication and accounting packets. The Called Station ID attribute can be used to classify users to different groups based on the attribute value. The command is applicable only for the Called Station and not for the Calling Station.

You cannot send only the SSID as the Called-Station-ID, you can only combine the SSID with either the access point MAC address or the access point name.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
7.6	The **ap-ethmac-only** and **ap-ethmac-ssid** keywords were added to support the access point's Ethernet MAC address. The **ap-label-address** and **ap-label-address-ssid** keywords were added.
8.0	This command supports both IPv4 and IPv6 address formats.
8.3	The **ap-mac-ssid-ap-group** keyword was added.

The following example shows how to configure the call station ID type to use the IP address:

```
(Cisco Controller) > config radius callStationIdType ipaddr
```

The following example shows how to configure the call station ID type to use the system's MAC address:

```
(Cisco Controller) > config radius callStationIdType macaddr
```

The following example shows how to configure the call station ID type to use the access point's MAC address:

```
(Cisco Controller) > config radius callStationIdType ap-macaddr-only
```

config radius dns

To retrieve the RADIUS IP information from a DNS server, use the **config radius dns** command.

config radius dns {**global** *port* {*ascii* | *hex*} *secret* | **query***url timeout* | **serverip** *ip_address* | **disable** | **enable**}

Syntax Description

global	Configures the global port and secret to retrieve the RADIUS IP information from a DNS server.
port	Port number for authentication. The range is from 1 to 65535. All the DNS servers should use the same authentication port.
ascii	Format of the shared secret that you should set to ASCII.
hex	Format of the shared secret that you should set to hexadecimal.
secret	RADIUS server login secret.
query	Configures the fully qualified domain name (FQDN) of the RADIUS server and DNS timeout.
url	FQDN of the RADIUS server. The FQDN can be up to 63 case-sensitive, alphanumeric characters.
timeout	Maximum time that the Cisco WLC waits for, in days, before timing out the request and resending it. The range is from 1 to 180.
serverip	Configures the DNS server IP address.
ip_address	DNS server IP address.
disable	Disables the RADIUS DNS feature. By default, this feature is disabled.
enable	Enables the Cisco WLC to retrieve the RADIUS IP information from a DNS server. When you enable a DNS query, the static configurations are overridden, that is, the DNS list overrides the static AAA list.

Command Default

You cannot configure the global port and secret to retrieve the RADIUS IP information.

Command History

Release	Modification
7.5	This command was introduced.

Usage Guidelines

The accounting port is derived from the authentication port. All the DNS servers should use the same secret.

The following example shows how to enable the RADIUS DNS feature on the Cisco WLC:

```
(Cisco Controller) > config radius dns enable
```

config radius fallback-test

To configure the RADIUS server fallback behavior, use the **config radius fallback-test** command.

config radius fallback-test mode {**off** | **passive** | **active**} | **username** *username*} | {**interval** *interval*}

Syntax Description

mode	Specifies the mode.
off	Disables RADIUS server fallback.
passive	Causes the controller to revert to a preferable server (with a lower server index) from the available backup servers without using extraneous probe messages. The controller ignores all inactive servers for a time period and retries later when a RADIUS message needs to be sent.
active	Causes the controller to revert to a preferable server (with a lower server index) from the available backup servers by using RADIUS probe messages to proactively determine whether a server that has been marked inactive is back online. The controller ignores all inactive servers for all active RADIUS requests.
username	Specifies the username.
username	Username. The username can be up to 16 alphanumeric characters.
interval	Specifies the probe interval value.
interval	Probe interval. The range is 180 to 3600.

Command Default

The default probe interval is 300.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to disable the RADIUS accounting server fallback behavior:

```
(Cisco Controller) > config radius fallback-test mode off
```

The following example shows how to configure the controller to revert to a preferable server from the available backup servers without using the extraneous probe messages:

```
(Cisco Controller) > config radius fallback-test mode passive
```

The following example shows how to configure the controller to revert to a preferable server from the available backup servers by using RADIUS probe messages:

```
(Cisco Controller) > config radius fallback-test mode active
```

Related Commands

config advanced probe filter

config advanced probe limit

show advanced probe

show radius acct statistics

config radius ext-source-ports

To configure support for extended source ports in the RADIUS servers, use the **config radius ext-source-ports** command.

config radius ext-source-ports { **enable** | **disable** }

Syntax Description

enable	Enables Radius source port support.
disable	Disables Radius source port support.

Command Default

None

Command Modes

Config

Command History

Release	Modification
8.1	This command was introduced.

The following example shows how to enable the extended source ports in the RADIUS servers:

```
config radius ext-source-ports enable
```

config radius acct retransmit-timeout

To change the default transmission timeout for a RADIUS accounting server for the Cisco wireless LAN controller, use the **config radius acct retransmit-timeout** command.

config radius acct retransmit-timeout *index timeout*

Syntax Description

index	RADIUS server index.
timeout	Number of seconds (from 2 to 30) between retransmissions.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure retransmission timeout value 5 seconds between the retransmission:

```
(Cisco Controller) > config radius acct retransmit-timeout 5
```

Related Commands

show radius acct statistics

config radius auth mgmt-retransmit-timeout

To configure a default RADIUS server retransmission timeout for management users, use the **config radius auth mgmt-retransmit-timeout** command.

config radius auth mgmt-retransmit-timeout *index retransmit-timeout*

Syntax Description

index	RADIUS server index.
retransmit-timeout	Timeout value. The range is from 1 to 30 seconds.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure a default RADIUS server retransmission timeout for management users:

```
(Cisco Controller) > config radius auth mgmt-retransmit-timeout 1 10
```

Related Commands

config radius auth management

config radius auth retransmit-timeout

To change a default transmission timeout for a RADIUS authentication server for the Cisco wireless LAN controller, use the **config radius auth retransmit-timeout** command.

config radius auth retransmit-timeout *index timeout*

Syntax Description

index	RADIUS server index.
timeout	Number of seconds (from 2 to 30) between retransmissions.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure a retransmission timeout of 5 seconds for a RADIUS authentication server:

```
(Cisco Controller) > config radius auth retransmit-timeout 5
```

Related Commands

show radius auth statistics

config radius auth retransmit-timeout

To configure a retransmission timeout value for a RADIUS accounting server, use the **config radius auth server-timeout** command.

config radius auth retransmit-timeout *index timeout*

Syntax Description

index	RADIUS server index.
timeout	Timeout value. The range is from 2 to 30 seconds.

Command Default

The default timeout is 2 seconds.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure a server timeout value of 2 seconds for RADIUS authentication server index 10:

```
(Cisco Controller) > config radius auth retransmit-timeout 2 10
```

Related Commands

show radius auth statistics

show radius summary

config redundancy interface address peer-service-port

To configure the service port IP and netmask of the peer or standby controller, use the **config redundancy interface address peer-service-port** command.

config redundancy interface address peer-service-port *ip_address netmask*

Syntax Description

ip_address	IP address of the peer service port.
netmask	Netmask of the peer service port.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

You can configure this command only from the Active controller. For the HA feature, the service port configurations are made per controller. You will loose these configurations if you change the mode from HA to non-HA and vice-versa.

The following example shows how to configure the service port IP and netmask of the peer or standby controller:

```
(Cisco Controller) >config redundancy interface address peer-service-port 11.22.44.55
```

config redundancy mobilitymac

To configure the High Availability mobility MAC address to be used as an identifier, use the **config redundancy mobilitymac** command.

config redundancy mobilitymac *mac_address*

Syntax Description

mac_address	MAC address that is an identifier for the active and standby controller pair.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

From Release 8.0.132.0 onwards, mobility MAC configuration is no longer present in the uploaded configuration. Therefore, if you download this configuration file back to the controller, you must add the **config redundancy mobilitymac** *mac_address*command in the config file before download.

Examples

The following example shows how to configure the High Availability mobility MAC address:

```
(Cisco Controller) >config redundancy mobilitymac ff:ff:ff:ff:ff:ff
```

config redundancy mode

To enable or disable redundancy or High Availability (HA), use the **config redundancy mode** command.

config redundancy mode {**sso** | **none**}

Syntax Description

sso	Enables a stateful switch over (SSO) or hot standby redundancy mode.
none	Disables redundancy mode.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

You must configure local and peer redundancy management IP addresses before you configure redundancy.

The following example shows how to enable redundancy:

```
(Cisco Controller) >config redundancy mode sso
```

config redundancy peer-route

To configure the route configurations of the peer or standby controller, use the **config redundancy peer-route** command.

config redundancy peer-route {**add** | **delete**} *network_ip_address netmask gateway*

Syntax Description

add	Adds a network route.
delete	Deletes a network route specific to standby controller.
network_ip_address	Network IP address.
netmask	Subnet mask of the network.
gateway	IP address of the gateway for the route network.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

You can configure this command only from the Active controller. For the HA feature, the service port configurations are made per controller. You will lose these configurations if you change the mode from HA to non-HA and vice-versa.

The following example shows how to configure route configurations of a peer or standby controller.

```
(Cisco Controller) >config redundancy peer-route add 10.1.1.0 255.255.255.0 10.1.1.1
```

config redundancy timer keep-alive-timer

To configure the keep-alive timeout value, use the **config redundancy timer keep-alive-timer** command.

config redundancy timer keep-alive-timer *milliseconds*

Syntax Description

milliseconds	Keep-alive timeout value in milliseconds. The range is from 100 to 400 milliseconds.

Command Default

The default keep-alive timeout value is 100 milliseconds.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the keep-alive timeout value:

```
(Cisco Controller) >config redundancy timer keep-alive-timer 200
```

config redundancy timer peer-search-timer

To configure the peer search timer, use the **config redundancy timer peer-search-timer** command.

config redundancy timer peer-search-timer *seconds*

Syntax Description

seconds	Value of the peer search timer in seconds. The range is from 60 to 180 secs.

Command Default

The default value of the peer search timer is 120 seconds.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

You can use this command to configure the boot up role negotiation timeout value in seconds.

The following example shows how to configure the redundancy peer search timer:

```
(Cisco Controller) >config redundancy timer peer-search-timer 100
```

config redundancy unit

To configure a Cisco WLC as a primary or secondary WLC, use the **config redundancy unit** command.

config redundancy unit {**primary** | **secondary**}

Syntax Description

primary	Configures the Cisco WLC as the primary WLC.
secondary	Configures the Cisco WLC as the secondary WLC.

Command Default

The default state is as the primary WLC.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

When you configure a Cisco WLC as the secondary WLC, it becomes the HA Stakable Unit (SKU) without any valid AP licenses.

The following example shows how to configure a Cisco WLC as the primary WLC:

```
(Cisco Controller) >config redundancy unit primary
```

config remote-lan

To configure a remote LAN, use the **config remote-lan** command.

config remote-lan {**enable** | **disable**} {*remote-lan-id* | **all**}

Syntax Description

enable	Enables a remote LAN.
disable	Disables a remote LAN.
remote-lan-id	Remote LAN identifier. Valid values are between 1 and 512.
all	Configures all wireless LANs.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable a remote LAN with ID 2:

```
(Cisco Controller) >config remote-lan enable 2
```

config remote-lan aaa-override

To configure user policy override through AAA on a remote LAN, use the **config remote-lan aaa-override** command.

config remote-lan aaa-override {**enable** | **disable**} *remote-lan-id*

Syntax Description

enable	Enables user policy override through AAA on a remote LAN.
disable	Disables user policy override through AAA on a remote LAN.
remote-lan-id	Remote LAN identifier. Valid values are between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable user policy override through AAA on a remote LAN where the remote LAN ID is 2:

```
(Cisco Controller) >config remote-lan aaa-override enable 2
```

config remote-lan acl

To specify an access control list (ACL) for a remote LAN, use the **config remote-lan acl** command.

config remote-lan acl *remote-lan-id acl_name*

Syntax Description

remote-lan-id	Remote LAN identifier. Valid values are between 1 and 512.
acl_name	ACL name. **Note** Use the **show acl summary** command to know the ACLs available.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to specify ACL1 for a remote LAN whose ID is 2:

```
(Cisco Controller) >config remote-lan acl 2 ACL1
```

config remote-lan apgroup

To add an access point (AP) group to remote LAN IEEE 802.1X, use the **config remote-lan apgroup** command.

config remote-lan apgroup add *apgroup-name description*

Syntax Description

add	Creates a new AP group.
apgroup-name	Name of an AP group to configure.
description	(Optional) Description of the AP group.

Command Default

None

Command Modes

Controller Configuration

Command History

Release	Modification
8.4	This command was introduced.

Usage Guidelines

Example

The following example shows how to add an AP group to remote LAN IEEE 802.1X:

```
(Cisco Controller) > config remote-lan apgroup add testap
```

config remote-lan create

To configure a new remote LAN connection, use the **config remote-lan create** command.

config remote-lan create *remote-lan-id name*

Syntax Description

remote-lan-id	Remote LAN identifier. Valid values are between 1 and 512.
name	Remote LAN name. Valid values are up to 32 alphanumeric characters.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure a new remote LAN, MyRemoteLAN, with the LAN ID as 3:

```
(Cisco Controller) >config remote-lan create 3 MyRemoteLAN
```

config remote-lan custom-web

To configure web authentication for a remote LAN, use the **config remote-lan custom-web** command.

config remote-lan custom-web {**ext-webauth-url** *URL* } | **global** {**enable** | **disable**} | **login-page** *page-name* | **loginfailure-page** {*page-name* | **none**} | **logout-page** {*page-name* | **none**} | **webauth-type** {**internal** | **customized** | **external**} } *remote-lan-id*

Syntax Description

ext-webauth-url	Configures an external web authentication URL.
URL	Web authentication URL for the Login page.
global	Configures the global status for the remote LAN.
enable	Enables the global status for the remote LAN.
disable	Disables the global status for the remote LAN.
login-page	Configures a login page.
page-name	Login page name.
none	Configures no login page.
logout-page	Configures a logout page.
none	Configures no logout page.
webauth-type	Configures the web authentication type for the remote LAN.
internal	Displays the default login page.
customized	Displays a downloaded login page.
external	Displays a login page that is on an external server.
name	Remote LAN name. Valid values are up to 32 alphanumeric characters.
remote-lan-id	Remote LAN identifier. Valid values are from 1 to 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Follow these guidelines when you use the **config remote-lan custom-web** command:

- When you configure the external Web-Auth URL, do the following:
  - Ensure that Web-Auth or Web-Passthrough Security is in enabled state. To enable Web-Auth, use the **config remote-lan security web-auth enable** command. To enable Web-Passthrough, use the **config remote-lan security web-passthrough enable** command.

- Ensure that the global status of the remote LAN is in disabled state. To enable the global status of the remote LAN, use the **config remote-lan custom-web global disable** command.
- Ensure that the remote LAN is in disabled state. To disable a remote LAN, use the **config remote-lan disable** command.

- When you configure the Web-Auth type for the remote LAN, do the following:
  - When you configure a customized login page, ensure that you have a login page configured. To configure a login page, use the **config remote-lan custom-web login-page** command.
  - When you configure an external login page, ensure that you have configured preauthentication ACL for external web authentication to function.

The following example shows how to configure an external web authentication URL for a remote LAN with ID 3:

```
(Cisco Controller) >config remote-lan custom-web ext-webauth-url
http://www.AuthorizationURL.com/ 3
```

The following example shows how to enable the global status of a remote LAN with ID 3:

```
(Cisco Controller) >config remote-lan custom-web global enable 3
```

The following example shows how to configure the login page for a remote LAN with ID 3:

```
(Cisco Controller) >config remote-lan custom-web login-page custompage1 3
```

The following example shows how to configure a web authentication type with the default login page for a remote LAN with ID 3:

```
(Cisco Controller) >config remote-lan custom-web webauth-type internal 3
```

config remote-lan delete

To delete a remote LAN connection, use the **config remote-lan delete** command.

config remote-lan delete *remote-lan-id*

Syntax Description

remote-lan-id	Remote LAN identifier. Valid values are between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to delete a remote LAN with ID 3:

```
(Cisco Controller) >config remote-lan delete 3
```

config remote-lan dhcp_server

To configure a dynamic host configuration protocol (DHCP) server for a remote LAN, use the **config remote-lan dhcp_server** command.

config remote-lan dhcp_server *remote-lan-id ip_address*

Syntax Description

remote-lan-id	Remote LAN identifier. Valid values are between 1 and 512.
ip_addr	IPv4 address of the override DHCP server.

Command Default

0.0.0.0 is set as the default interface value.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports only IPv4 address format.

The following example shows how to configure a DHCP server for a remote LAN with ID 3:

```
(Cisco Controller) >config remote-lan dhcp_server 3 209.165.200.225
```

Related Commands

show remote-lan

config remote-lan exclusionlist

To configure the exclusion list timeout on a remote LAN, use the **config remote-lan exclusionlist** command.

config remote-lan exclusionlist *remote-lan-id* {*seconds* | **disabled** | **enabled**}

Syntax Description

remote-lan-id	Remote LAN identifier. Valid values are between 1 and 512.
seconds	Exclusion list timeout in seconds. A value of 0 requires an administrator override.
disabled	Disables exclusion listing.
enabled	Enables exclusion listing.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the exclusion list timeout to 20 seconds on a remote LAN with ID 3:

```
(Cisco Controller) >config remote-lan exclusionlist 3 20
```

config remote-lan host-mode

To configure a host mode for remote LAN IEEE 802.1X, use the **config remote-lan host-mode** command.

config remote-lan host-mode {**singlehost** | **multihost** } *remote-lan-id*

Syntax Description

singlehost	Configures the remote LAN single-host mode.
multihost	Configures the remote LAN multi-host mode.
remote-lan-id	WLAN identifier. The range is from 1 to 512.

Command Default

None

Command Modes

Controller Configuration

Command History

Release	Modification
8.4	This command was introduced.

Example

The following example shows how to configure the host mode as single for remote LAN IEEE 802.1X:

```
(Cisco Controller) > config remote-lan host-mode singlehost 1
```

config remote-lan interface

To configure an interface for a remote LAN, use the **config remote-lan interface** command.

config remote-lan interface *remote-lan-id interface_name*

Syntax Description

remote-lan-id	Remote LAN identifier. Valid values are between 1 and 512.
interface_name	Interface name. **Note** Interface name should not be in upper case characters.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure an interface myinterface for a remote LAN with ID 3:

```
(Cisco Controller) >config remote-lan interface 3 myinterface
```

config remote-lan ldap

To configure a remote LAN's LDAP servers, use the **config remote-lan ldap** command.

config remote-lan ldap {**add** | **delete**} *remote-lan-id index*

Syntax Description

add	Adds a link to a configured LDAP server (maximum of three).
delete	Deletes a link to a configured LDAP server.
remote-lan-id	Remote LAN identifier. Valid values are between 1 and 512.
index	LDAP server index.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to add an LDAP server with the index number 10 for a remote LAN with ID 3:

```
(Cisco Controller) >config remote-lan ldap add 3 10
```

config remote-lan mac-filtering

To configure MAC filtering on a remote LAN, use the **config remote-lan mac-filtering** command.

config remote-lan mac-filtering {**enable** | **disable**} *remote-lan-id*

Syntax Description

enable	Enables MAC filtering on a remote LAN.
disable	Disables MAC filtering on a remote LAN.
remote-lan-id	Remote LAN identifier. Valid values are between 1 and 512.

Command Default

MAC filtering on a remote LAN is enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to disable MAC filtering on a remote LAN with ID 3:

```
(Cisco Controller) >config remote-lan mac-filtering disable 3
```

config remote-lan mab

To configure MAC Authentication Bypass (MAB) authentication support for AP Port LAN clients, use the **config remote-lan mab** command.

config remote-lan mab {**enable** | **disable**} *remote-lan-id*

Syntax Description

enable	Enables MAB authentication support.
disable	Disables MAB authentication support.
remote-lan-id	WLAN Identifier. The valid range is between 1 and 512.

Command Default

None

Command Modes

Controller Configuration

Command History

Release	Modification
8.4	This command was introduced.

Example

The following example shows how to enable MAB authentication support for AP Port LAN clients:

```
(Cisco Controller) >config remote-lan mab enable 8
```

config remote-lan max-associated-clients

To configure the maximum number of client connections on a remote LAN, use the **config remote-lan max-associated-clients** command.

config remote-lan max-associated-clients *remote-lan-id max-clients*

Syntax Description

remote-lan-id	Remote LAN identifier. Valid values are between 1 and 512.
max-clients	Configures the maximum number of client connections on a remote LAN.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure 10 client connections on a remote LAN with ID 3:

```
(Cisco Controller) >config remote-lan max-associated-clients 3 10
```

config remote-lan pre-auth

To configure a preauthentication VLAN for RLAN IEEE 802.1X, use the **config remote-lan pre-auth** command.

config remote-lan pre-auth {**enable** | **disable**} *remote-lan-id* **vlan** *vlan-id*

Syntax Description

enable	Enables RLAN preauthentication.
disable	Disables RLAN preauthentication.
remote-lan-id	WLAN identifier. The range is from 1 to 512.
vlan	Configures preauthentication VLAN for RLAN IEEE 802.1X.
vlan-id	Remote LAN preauthentication VLAN identifier.

Command Default

None

Command Modes

(Controller Configuration)

Command History

Release	Modification
8.4	This command was introduced.

Example

The following example shows how to enable preauthentication VLAN for remote LAN IEEE 802.1X:

```
(Cisco Controller) > config remote-lan pre-auth enable 1 vlan vlan1
```

config remote-lan radius_server

To configure the RADIUS servers on a remote LAN, use the **config remote-lan radius_server** command.

config remote-lan radius_server {**acct** {{**add** | **delete**} *server-index* | {**enable** | **disable**} | **interim-update** {*interval* | **enable** | **disable**}} | **auth** {{**add** | **delete**} *server-index* | {**enable** | **disable** }} | **overwrite-interface** {**enable** | **disable**}} *remote-lan-id*

Syntax Description

acct	Configures a RADIUS accounting server.
add	Adds a link to a configured RADIUS server.
delete	Deletes a link to a configured RADIUS server.
remote-lan-id	Remote LAN identifier. Valid values are between 1 and 512.
server-index	RADIUS server index.
enable	Enables RADIUS accounting for this remote LAN.
disable	Disables RADIUS accounting for this remote LAN.
interim-update	Enables RADIUS accounting for this remote LAN.
interval	Accounting interim interval. The range is from 180 to 3600 seconds.
enable	Enables accounting interim update.
disable	Disables accounting interim update.
auth	Configures a RADIUS authentication server.
enable	Enables RADIUS authentication for this remote LAN.
disable	Disables RADIUS authentication for this remote LAN.
overwrite-interface	Configures a RADIUS dynamic interface for the remote LAN.
enable	Enables a RADIUS dynamic interface for the remote LAN.
disable	Disables a RADIUS dynamic interface for the remote LAN.

Command Default

The interim update interval is set to 600 seconds.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable RADIUS accounting for a remote LAN with ID 3:

```
(Cisco Controller) >config remote-lan radius_server acct enable 3
```

config remote-lan security

To configure security policy for a remote LAN, use the **config remote-lan security** command.

config remote-lan security {{**web-auth** {**enable** | **disable** | **acl** | **server-precedence**} *remote-lan-id* | {**web-passthrough** {**enable** | **disable** | **acl** | **email-input**} *remote-lan-id*}}

Syntax Description

web-auth	Specifies web authentication.
enable	Enables the web authentication settings.
disable	Disables the web authentication settings.
acl	Configures an access control list.
server-precedence	Configures the authentication server precedence order for web authentication users.
remote-lan-id	Remote LAN identifier. Valid values are between 1 and 512.
email-input	Configures the web captive portal using an e-mail address.
web-passthrough	Specifies the web captive portal with no authentication required.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.4	The **802.1X** keyword was added.

The following example shows how to configure the security web authentication policy for remote LAN ID 1:

```
(Cisco Controller) >config remote-lan security web-auth enable 1
```

config remote-lan session-timeout

To configure client session timeout, use the **config remote-lan session-timeout** command.

config remote-lan session-timeout *remote-lan-id seconds*

Syntax Description

remote-lan-id	Remote LAN identifier. Valid values are between 1 and 512.
seconds	Timeout or session duration in seconds. A value of zero is equivalent to no timeout.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the client session timeout to 6000 seconds for a remote LAN with ID 1:

```
(Cisco Controller) >config remote-lan session-timeout 1 6000
```

config remote-lan violation-mode

To configure the violation mode for remote LAN IEEE 802.1X, use the **config remote-lan violation-mode** command.

config remote-lan violation-mode {**protect** | **replace** | **shutdown**} *remote-lan-id*

Syntax Description

protect	Configures the remote LAN protect mode.
replace	Configures the remote LAN replace mode.
shutdown	Configures the remote LAN shutdown mode.
remote-lan-id	WLAN identifier. The range is from 1 to 512.

Command Default

None

Command Modes

Controller Configuration

Command History

Release	Modification
8.4	This command was introduced.

Usage Guidelines

Example

The following example shows how to configure the violation mode as protect for remote LAN IEEE 802.1X:

```
(Cisco Controller) > config remote-lan violation-mode protect 1
```

config remote-lan webauth-exclude

To configure web authentication exclusion on a remote LAN, use the **config remote-lan webauth-exclude** command.

config remote-lan webauth-exclude *remote-lan-id* {**enable** | **disable**}

Syntax Description

remote-lan-id	Remote LAN identifier. Valid values are between 1 and 512.
enable	Enables web authentication exclusion on the remote LAN.
disable	Disables web authentication exclusion on the remote LAN.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable web authentication exclusion on a remote LAN with ID 1:

```
(Cisco Controller) >config remote-lan webauth-exclude 1 enable
```

config rf-profile band-select

To configure the RF profile band selection parameters, use the **config rf-profile band-select** command.

config rf-profile band-select {**client-rssi** *rssi* | **cycle-count** *cycles* | **cycle-threshold** *value* | **expire** {**dual-band** *value* | **suppression** *value*} | **probe-response** {**enable** | **disable**}} *profile_name*

Syntax Description

client-rssi	Configures the client Received Signal Strength Indicator (RSSI) threshold for the RF profile.
rssi	Minimum RSSI for a client to respond to a probe. The range is from -20 to -90 dBm.
cycle-count	Configures the probe cycle count for the RF profile. The cycle count sets the number of suppression cycles for a new client.
cycles	Value of the cycle count. The range is from 1 to 10.
cycle-threshold	Configures the time threshold for a new scanning RF Profile band select cycle period. This setting determines the time threshold during which new probe requests from a client come in a new scanning cycle.
value	Value of the cycle threshold for the RF profile. The range is from 1 to 1000 milliseconds.
expire	Configures the expiration time of clients for band select.
dual-band	Configures the expiration time for pruning previously known dual-band clients. After this time elapses, clients become new and are subject to probe response suppression.
value	Value for a dual band. The range is from 10 to 300 seconds.
suppression	Configures the expiration time for pruning previously known 802.11b/g clients. After this time elapses, clients become new and are subject to probe response suppression.
value	Value for suppression. The range is from 10 to 200 seconds.
probe-response	Configures the probe response for a RF profile.
enable	Enables probe response suppression on clients operating in the 2.4-GHz band for a RF profile.
disable	Disables probe response suppression on clients operating in the 2.4-GHz band for a RF profile.
profile name	Name of the RF profile. The profile name can be up to 32 case-sensitive, alphanumeric characters.

Command Default

The default value for client RSSI is –80 dBm.

The default cycle count is 2.

The default cycle threshold is 200 milliseconds.

The default value for dual-band expiration is 60 seconds.

The default value for suppression expiration is 20 seconds.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

When you enable band select on a WLAN, the access point suppresses client probes on 2.4-GHz 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. Band selection can be used only with Cisco Aironet 1040, 1140, and 1250 Series and the 3500 series access points.

The following example shows how to configure the client RSSI:

```
(Cisco Controller) >config rf-profile band-select client-rssi -70
```

config rf-profile channel

To configure the RF profile DCA settings, use the **config rf-profile channel** command.

config rf-profile channel {**add** *chan profile name* | **delete** *chan profile name* | **foreign** {**enable** | **disable**} *profile name* | **chan-width** {**20** | **40** | **80**} *profile name*}

Syntax Description

add	Adds channel to the RF profile DCA channel list.
delete	Removes channel from the RF profile DCA channel list.
foreign	Configures the RF profile DCA foreign AP contribution.
chan-width	Configures the RF profile DCA channel width.
chan	Specifies channel number.
profile name	Specifies the name of the RF profile. The profile name can be up to 32 case-sensitive, alphanumeric characters.
enable	Enables foreign AP interference.
disable	Disables foreign AP interference.
{**20** | **40** | **80**}	Specifies RF Profile DCA channel width.

Command Default

None

Command History

Release	Modification
8.0	This command was introduced.

The following example shows how to add a channel to the RF profile DCA channel list:

```
(Cisco Controller) >config rf-profile channel add 40 admin1
```

The following example shows how to configure the RF profile DCA channel width:

```
(Cisco Controller) >config rf-profile channel chan-width 40 admin1
```

config rf-profile client-trap-threshold

To configure the threshold value of the number of clients that associate with an access point, after which an SNMP trap is sent to the controller, use the **config rf-profile client-trap-threshold** command.

config rf-profile client-trap-threshold *threshold profile_name*

Syntax Description

threshold	Threshold value of the number of clients that associate with an access point, after which an SNMP trap is sent to the controller. The range is from 0 to 200. Traps are disabled if the threshold value is configured as zero.
profile_name	Name of the RF profile. The profile name can be up to 32 case-sensitive, alphanumeric characters.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the threshold value of the number of clients that associate with an access point:

```
(Cisco Controller) >config rf-profile client-trap-threshold 150
```

config rf-profile create

To create a RF profile, use the **config rf-profile create** command.

config rf-profile create {**802.11a** | **802.11b/g**} *profile-name*

Syntax Description

802.11a	Configures the RF profile for the 2.4GHz band.
802.11b/g	Configures the RF profile for the 5GHz band.
profile-name	Name of the RF profile.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to create a new RF profile:

```
(Cisco Controller) >config rf-profile create 802.11a RFtestgroup1
```

config rf-profile fra client-aware

To configure the RF profile client-aware FRA feature, use the **config rf-profile fra client-aware** command.

config rf-profile fra client-aware {**client-reset** *percent rf-profile-name* | **client-select** *percent rf-profile-name* | **disable** *rf-profile-name* | **enable** *rf-profile-name*}

Syntax Description

client-reset	Configures the RF profile AP utilization threshold for radio to switch back to Monitor mode.
percent	Utilization percentage value ranges from 0 to 100. The default is 5%.
rf-profile-name	Name of the RF Profile.
client-select	Configures the RF profile utilization threshold for radio to switch to 5GHz.
percent	Utilization percentage value ranges from 0 to 100. The default is 50%.
disable	Disables the RF profile client-aware FRA feature.
enable	Enables the RF profile client-aware FRA feature.

Command Default

The default percent value for client-select and client-reset is 50% and 5% respectively.

Command History

Release	Modification
8.5	This command was introduced.

The following example shows how to configure the RF profile utilization threshold for redundant dual-band radios to switch back from 5GHz client-serving role to Monitor mode:

```
(Cisco Controller) >config rf-profile fra client-aware client-reset 15 profile1
```

The following example shows how to configure the RF profile utilization threshold for redundant dual-band radios to switch from Monitor mode to 5GHz client-serving role:

```
(Cisco Controller) >config rf-profile fra client-aware client-select 20 profile1
```

The following example shows how to disable the RF profile client-aware FRA feature:

```
(Cisco Controller) >config rf-profile fra client-aware disable profile1
```

The following example shows how to enable the RF profile client-aware FRA feature:

```
(Cisco Controller) >config rf-profile fra client-aware enable profile1
```

config rf-profile data-rates

To configure the data rate on a RF profile, use the **config rf-profile data-rates** command.

config rf-profile data-rates {**802.11a** | **802.11b** } {**disabled** | **mandatory** | **supported**} *data-rate profile-name*

Syntax Description

802.11a	Specifies 802.11a as the radio policy of the RF profile.
802.11b	Specifies 802.11b as the radio policy of the RF profile.
disabled	Disables a rate.
mandatory	Sets a rate to mandatory.
supported	Sets a rate to supported.
data-rate	802.11 operational rates, which are 1*, 2*, 5.5*, 6, 9, 11*, 12, 18, 24, 36, 48 and 54, where * denotes 802.11b only rates.
profile-name	Name of the RF profile.

Command Default

Default data rates for RF profiles are derived from the controller system defaults, the global data rate configurations. For example, if the RF profile's radio policy is mapped to 802.11a then the global 802.11a data rates are copied into the RF profiles at the time of creation.

The data rates set with this command are negotiated between the client and the Cisco wireless LAN controller. If the data rate is set to mandatory, the client must support it in order to use the network. If a data rate is set as supported by the Cisco wireless LAN controller, any associated client that also supports that rate may communicate with the Cisco lightweight access point using that rate. It is not required that a client is able to use all the rates marked supported in order to associate.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to set the 802.11b transmission of an RF profile at a mandatory rate at 12 Mbps:

```
(Cisco Controller) >config rf-profile 802.11b data-rates mandatory 12 RFGroup1
```

config rf-profile delete

To delete a RF profile, use the **config rf-profile delete** command.

config rf-profile delete *profile-name*

Syntax Description

profile-name	Name of the RF profile.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to delete a RF profile:

```
(Cisco Controller) >config rf-profile delete RFGroup1
```

config rf-profile description

To provide a description to a RF profile, use the **config rf-profile description** command.

config rf-profile description *description profile-name*

Syntax Description

description	Description of the RF profile.
profile-name	Name of the RF profile.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to add a description to a RF profile:

```
(Cisco Controller) >config rf-profile description This is a demo desciption RFGroup1
```

config rf-profile fra client-aware

To configure the RF profile client-aware FRA feature, use the **config rf-profile fra client-aware** command.

config rf-profile fra client-aware {**client-reset** *percent rf-profile-name* | **client-select** *percent rf-profile-name* | **disable** *rf-profile-name* | **enable** *rf-profile-name*}

Syntax Description

client-reset	Configures the RF profile AP utilization threshold for radio to switch back to Monitor mode.
percent	Utilization percentage value ranges from 0 to 100. The default is 5%.
rf-profile-name	Name of the RF Profile.
client-select	Configures the RF profile utilization threshold for radio to switch to 5GHz.
percent	Utilization percentage value ranges from 0 to 100. The default is 50%.
disable	Disables the RF profile client-aware FRA feature.
enable	Enables the RF profile client-aware FRA feature.

Command Default

The default percent value for client-select and client-reset is 50% and 5% respectively.

Command History

Release	Modification
8.5	This command was introduced.

The following example shows how to configure the RF profile utilization threshold for redundant dual-band radios to switch back from 5GHz client-serving role to Monitor mode:

```
(Cisco Controller) >config rf-profile fra client-aware client-reset 15 profile1
```

The following example shows how to configure the RF profile utilization threshold for redundant dual-band radios to switch from Monitor mode to 5GHz client-serving role:

```
(Cisco Controller) >config rf-profile fra client-aware client-select 20 profile1
```

The following example shows how to disable the RF profile client-aware FRA feature:

```
(Cisco Controller) >config rf-profile fra client-aware disable profile1
```

The following example shows how to enable the RF profile client-aware FRA feature:

```
(Cisco Controller) >config rf-profile fra client-aware enable profile1
```

config rf-profile load-balancing

To configure load balancing on an RF profile, use the **config rf-profile load-balancing** command.

config rf-profile load-balancing {**window** *clients* | **denial** *value*} *profile_name*

Syntax Description

window	Configures the client window for load balancing of an RF profile.
clients	Client window size that limits the number of client associations with an access point. The range is from 0 to 20. The default value is 5. The window size is part of the algorithm that determines whether an access point is too heavily loaded to accept more client associations: *load-balancing window + client associations on AP with lightest load = load-balancing threshold* Access points with more client associations than this threshold are considered busy, and clients can associate only to access points with client counts lower than the threshold. This window also helps to disassociate sticky clients.
denial	Configures the client denial count for load balancing of an RF profile.
value	Maximum number of association denials during load balancing. The range is from 1 to 10. The default value is 3. When a client tries to associate on a wireless network, it sends an association request to the access point. If the access point is overloaded and load balancing is enabled on the controller, the access point sends a denial to the association request. If there are no other access points in the range of the client, the client tries to associate the same access point again. After the maximum denial count is reached, the client is able to associate. Association attempts on an access point from any client before associating any AP is called a sequence of association. The default is 3.
profile_name	Name of the RF profile. The profile name can be up to 32 case-sensitive, alphanumeric characters.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the client window size for an RF profile:

```
(Cisco Controller) >config rf-profile load-balancing window 15
```

config rf-profile max-clients

To configure the maximum number of client connections per access point of an RF profile, use the **config rf-profile max-clients** commands.

config rf-profile max-clients *clients*

Syntax Description

clients	Maximum number of client connections per access point of an RF profile. The range is from 1 to 200.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

You can use this command to configure the maximum number of clients on access points that are in client dense areas, or serving high bandwidth video or mission critical voice applications.

The following example shows how to set the maximum number of clients at 50:

```
(Cisco Controller) >config rf-profile max-clients 50
```

config rf-profile multicast data-rate

To configure the minimum RF profile multicast data rate, use the **config rf-profile multicast data-rate** command.

config rf-profile multicast data-rate *value profile_name*

Syntax Description

value	Minimum RF profile multicast data rate. The options are 6, 9, 12, 18, 24, 36, 48, 54. Enter 0 to specify that access points will dynamically adjust the data rate.
profile_name	Name of the RF profile. The profile name can be up to 32 case-sensitive, alphanumeric characters.

Command Default

The minimum RF profile multicast data rate is 0.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to set the multicast data rate for an RF profile:

```
(Cisco Controller) >config rf-profile multicast data-rate 24
```

config rf-profile out-of-box

To create an out-of-box AP group consisting of newly installed access points, use the **config rf-profile out-of-box** command.

config rf-profile out-of-box {**enable** | **disable**}

Syntax Description

enable	Enables the creation of an out-of-box AP group. When you enable this command, the following occurs: • Newly installed access points that are part of the default AP group will be part of the out-of-box AP group and their radios will be switched off, which eliminates any RF instability caused by the new access points. • All access points that do not have a group name become part of the out-of-box AP group. • Special RF profiles are created per 802.11 band. These RF profiles have default-settings for all the existing RF parameters and additional new configurations.
disable	Disables the out-of-box AP group. When you disable this feature, only the subscription of new APs to the out-of-box AP group stops. All APs that are subscribed to the out-of-box AP group remain in this AP group. You can move APs to the default group or a custom AP group upon network convergence.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

When an out-of-box AP associates with the controller for the first time, it will be redirected to a special AP group and the RF profiles applicable to this AP Group will control the radio admin state configuration of the AP. You can move APs to the default group or a custom group upon network convergence.

The following example shows how to enable the creation of an out-of-box AP group:

```
(Cisco Controller) >config rf-profile out-of-box enable
```

config rf-profile rx-sop threshold

To configure high, medium or low Rx SOP threshold values for each 802.11 band, use the **config rf-profile rx-sop threshold** command.

config rf-profile rx-sop threshold {**high** | **medium** | **low** | **auto**} *profile_name*

Syntax Description

high	Configures the high Rx SOP threshold value for an RF profile.
medium	Configures the medium Rx SOP threshold value for an RF profile.
low	Configures the low Rx SOP threshold value for an RF profile.
auto	Configures an auto Rx SOP threshold value for an RF profile. When you choose auto, the access point determines the best Rx SOP threshold value.
profile_name	RF profile on which the Rx SOP threshold value will be configured.

Command Default

The default Rx SOP threshold option is auto.

Command History

Release	Modification
8.0	This command was introduced.

The following example shows how to configure the high Rx SOP threshold value on an RF profile:

```
(Cisco Controller) > config 802.11 rx-sop threshold high T1a
```

config rf-profile trap-threshold

To configure the RF profile trap threshold, use the **config rf-profile trap-threshold** command.

config rf-profile trap-threshold {**clients** *clients profile name* | **interference** *percent profile name* | **noise** *dBm profile name* | **utilization** *percent profile name*}

Syntax Description

clients	Configures the RF profile trap threshold for clients.
clients	The number of clients on an access point's radio for the trap is between 1 and 200. The default is 12 clients.
profile name	Specifies the name of the RF profile. The profile name can be up to 32 case-sensitive, alphanumeric characters.
interference	Configures the RF profile trap threshold for interference.
percent	The percentage of interference threshold for the trap is from 0 to 100 %. The default is 10 %.
noise	Configures the RF profile trap threshold for noise.
dBM	The level of noise threshold for the trap is from -127 to 0 dBm. The default is -17 dBm.
utilization	Configures the RF profile trap threshold for utilization.
percent	The percentage of bandwidth being used by an access point threshold for the trap is from 0 to 100 %. The default is 80 %.

Command Default

None

Command History

Release	Modification
8.0	This command was introduced.

The following example shows how to configure the RF profile trap threshold for clients:

```
(Cisco Controller) >config rf-profile trap-threshold clients 50 admin1
```

config rf-profile tx-power-control-thresh-v1

To configure Transmit Power Control version1 (TPCv1) to an RF profile, use the **config rf-profile tx-power-control-thresh-v1** command.

config rf-profile tx-power-control-thresh-v1 *tpc-threshold profile_name*

Syntax Description

tpc-threshold	TPC threshold.
profile-name	Name of the RF profile.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure TPCv1 on an RF profile:

```
(Cisco Controller) >config rf-profile tx-power-control-thresh-v1 RFGroup1
```

config rf-profile tx-power-control-thresh-v2

To configure Transmit Power Control version 2 (TPCv2) to an RF profile, use the **config rf-profile tx-power-control-thresh-v2** command.

config rf-profile tx-power-control-thresh-v2 *tpc-threshold profile-name*

Syntax Description

tpc-threshold	TPC threshold.
profile-name	Name of the RF profile.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure TPCv2 on an RF profile:

```
(Cisco Controller) >config rf-profile tx-power-control-thresh-v2 RFGroup1
```

config rf-profile tx-power-max

To configure maximum auto-rf to an RF profile, use the **config rf-profile tx-power-max** command.

config rf-profile *tx-power-max profile-name*

Syntax Description

tx-power-max	Maximum auto-rf tx power.
profile-name	Name of the RF profile.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure tx-power-max on an RF profile:

```
(Cisco Controller) >config rf-profile tx-power-max RFGroup1
```

config rf-profile tx-power-min

To configure minimum auto-rf to an RF profile, use the **config rf-profile tx-power-min** command.

config rf-profile tx-power-min *tx-power-min profile-name*

Syntax Description

tx-power-min	Minimum auto-rf tx power.
profile-name	Name of the RF profile.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure tx-power-min on an RF profile:

```
(Cisco Controller) >config rf-profile tx-power-min RFGroup1
```

config rogue ap timeout

To specify the number of seconds after which the rogue access point and client entries expire and are removed from the list, use the **config rogue ap timeout** command.

config rogue ap timeout *seconds*

Syntax Description

seconds	Value of 240 to 3600 seconds (inclusive), with a default value of 1200 seconds.

Command Default

The default number of seconds after which the rogue access point and client entries expire is 1200 seconds.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to set an expiration time for entries in the rogue access point and client list to 2400 seconds:

```
(Cisco Controller) > config rogue ap timeout 2400
```

Related Commands

config rogue ap classify

config rogue ap friendly

config rogue ap rldp

config rogue ap ssid

config rogue rule

config trapflags rogueap

show rogue ap clients

show rogue ap detailed

show rogue ap summary

show rogue ap friendly summary

show rogue ap malicious summary

show rogue ap unclassified summary

show rogue ignore-list

show rogue rule detailed

show rogue rule summary

config rogue adhoc

To globally or individually configure the status of an Independent Basic Service Set (IBSS or *ad-hoc*) rogue access point, use the **config rogue adhoc** command.

config rogue adhoc {**enable** | **disable** | **external** *rogue_MAC* | **alert** {*rogue_MAC* | **all**} | **auto-contain** [*monitor_ap*] | **contain** *rogue_MAC 1234_aps* | }

config rogue adhoc {**delete** {**all** | **mac-address** *mac-address*} | **classify** {**friendly state** {**external** | **internal**} *mac-address* | **malicious state** {**alert** | **contain**} *mac-address* | **unclassified state** {**alert** | **contain** } *mac-address*}

Syntax Description

enable	Globally enables detection and reporting of ad-hoc rogues.
disable	Globally disables detection and reporting of ad-hoc rogues.
external	Configure external state on the rogue access point that is outside the network and poses no threat to WLAN security. The controller acknowledges the presence of this rogue access point.
rogue_MAC	MAC address of the ad-hoc rogue access point.
alert	Generates an SMNP trap upon detection of the ad-hoc rogue, and generates an immediate alert to the system administrator for further action.
all	Enables alerts for all ad-hoc rogue access points.
auto-contain	Contains all wired ad-hoc rogues detected by the controller.
monitor_ap	(Optional) IP address of the ad-hoc rogue access point.
contain	Contains the offending device so that its signals no longer interfere with authorized clients.
1234_aps	Maximum number of Cisco access points assigned to actively contain the ad-hoc rogue access point (1 through 4, inclusive).
delete	Deletes ad-hoc rogue access points.
all	Deletes all ad-hoc rogue access points.
mac-address	Deletes ad-hoc rogue access point with the specified MAC address.
mac-address	MAC address of the ad-hoc rogue access point.

classify	Configures ad-hoc rogue access point classification.
friendly state	Classifies ad-hoc rogue access points as friendly.
internal	Configures alert state on rogue access point that is inside the network and poses no threat to WLAN security. The controller trusts this rogue access point.
malicious state	Classifies ad-hoc rogue access points as malicious.
alert	Configures alert state on the rogue access point that is not in the neighbor list or in the user configured friendly MAC list. The controller forwards an immediate alert to the system administrator for further action.
contain	Configures contain state on the rogue access point. Controller contains the offending device so that its signals no longer interfere with authorized clients.
unclassified state	Classifies ad-hoc rogue access points as unclassified.

Command Default

The default for this command is **enabled** and is set to **alert**. The default for auto-containment is **disabled**.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

The controller continuously monitors all nearby access points and automatically discovers and collects information on rogue access points and clients. When the controller discovers a rogue access point, it uses RLDP to determine if the rogue is attached to your wired network.

Note RLDP is not supported for use with Cisco autonomous rogue access points. These access points drop the DHCP Discover request sent by the RLDP client. Also, RLDP is not supported if the rogue access point channel requires dynamic frequency selection (DFS).

When you enter any of the containment commands, the following warning appears:

```
Using this feature may have legal consequences. Do you want to continue? (y/n) :
```

The 2.4- and 5-GHz frequencies in the Industrial, Scientific, and Medical (ISM) band are open to the public and can be used without a license. As such, containing devices on another party's network could have legal consequences.

Enter the **auto-contain** command with the *monitor_ap* argument to monitor the rogue access point without containing it. Enter the **auto-contain** command without the optional *monitor_ap* to automatically contain all wired ad-hoc rogues detected by the controller.

The following example shows how to enable the detection and reporting of ad-hoc rogues:

```
(Cisco Controller) > config rogue adhoc enable
```

The following example shows how to enable alerts for all ad-hoc rogue access points:

```
(Cisco Controller) > config rogue adhoc alert all
```

The following example shows how to classify an ad-hoc rogue access point as friendly and configure external state on it:

```
(Cisco Controller) > config rogue adhoc classify friendly state internal 11:11:11:11:11:11
```

Related Commands

config rogue auto-contain level

show rogue ignore-list

show rogue rule detailed

show rogue rule summary

config rogue ap classify

To classify the status of a rogue access point, use the **config rogue ap classify** command.

config rogue ap classify {**friendly state** {**internal** | **external**} *ap_mac* }

config rogue ap classify {**malicious** | **unclassified**} **state** {**alert** | **contain**} *ap_mac*

Syntax Description

friendly	Classifies a rogue access point as friendly.
state	Specifies a response to classification.
internal	Configures the controller to trust this rogue access point.
external	Configures the controller to acknowledge the presence of this access point.
ap_mac	MAC address of the rogue access point.
malicious	Classifies a rogue access point as potentially malicious.
unclassified	Classifies a rogue access point as unknown.
alert	Configures the controller to forward an immediate alert to the system administrator for further action.
contain	Configures the controller to contain the offending device so that its signals no longer interfere with authorized clients.

Command Default

These commands are disabled by default. Therefore, all unknown access points are categorized as **unclassified** by default.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

A rogue access point cannot be moved to the unclassified class if its current state is contain.

When you enter any of the containment commands, the following warning appears: “Using this feature may have legal consequences. Do you want to continue?” The 2.4- and 5-GHz frequencies in the Industrial, Scientific, and Medical (ISM) band are open to the public and can be used without a license. As such, containing devices on another party’s network could have legal consequences.

The following example shows how to classify a rogue access point as friendly and can be trusted:

```
(Cisco Controller) > config rogue ap classify friendly state internal 11:11:11:11:11:11
```

The following example shows how to classify a rogue access point as malicious and to send an alert:

```
(Cisco Controller) > config rogue ap classify malicious state alert 11:11:11:11:11:11
```

The following example shows how to classify a rogue access point as unclassified and to contain it:

```
(Cisco Controller) > config rogue ap classify unclassified state contain 11:11:11:11:11:11
```

Related Commands

config rogue adhoc
config rogue ap friendly
config rogue ap rldp
config rogue ap ssid
config rogue ap timeout
config rogue ap valid-client
config rogue client
config trapflags rogueap
show rogue ap clients
show rogue ap detailed
show rogue ap summary
show rogue ap friendly summary
show rogue ap malicious summary
show rogue ap unclassified summary
show rogue client detailed
show rogue client summary
show rogue ignore-list
show rogue rule detailed
show rogue rule summary

config rogue ap friendly

To add a new friendly access point entry to the friendly MAC address list, or delete an existing friendly access point entry from the list, use the **config rogue ap friendly** command.

config rogue ap friendly {**add** | **delete**} *ap_mac*

Syntax Description

add	Adds this rogue access point from the friendly MAC address list.
delete	Deletes this rogue access point from the friendly MAC address list.
ap_mac	MAC address of the rogue access point that you want to add or delete.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to add a new friendly access point with MAC address 11:11:11:11:11:11 to the friendly MAC address list.

```
(Cisco Controller) > config rogue ap friendly add 11:11:11:11:11:11
```

Related Commands

config rogue adhoc

config rogue ap classify

config rogue ap rldp

config rogue ap ssid

config rogue ap timeout

config rogue ap valid-client

config rogue client

config trapflags rogueap

show rogue ap clients

show rogue ap detailed

show rogue ap summary

show rogue ap friendly summary

show rogue ap malicious summary

show rogue ap unclassified summary

show rogue client detailed

show rogue client summary

show rogue ignore-list

show rogue rule detailed

show rogue rule summary

config rogue ap rldp

To enable, disable, or initiate the Rogue Location Discovery Protocol (RLDP), use the **config rogue ap rldp** command.

config rogue ap rldp enable {**alarm-only** | **auto-contain**} [*monitor_ap_only*]

config rogue ap rldp initiate *rogue_mac_address*

config rogue ap rldp disable

Syntax Description

alarm-only	When entered without the optional argument *monitor_ap_only*, enables RLDP on all access points.
auto-contain	When entered without the optional argument *monitor_ap_only*, automatically contains all rogue access points.
monitor_ap_only	(Optional) RLDP is enabled (when used with **alarm-only** keyword), or automatically contained (when used with **auto-contain** keyword) is enabled only on the designated monitor access point.
initiate	Initiates RLDP on a specific rogue access point.
rogue_mac_address	MAC address of specific rogue access point.
disable	Disables RLDP on all access points.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

When you enter any of the containment commands, the following warning appears: “Using this feature may have legal consequences. Do you want to continue?” The 2.4- and 5-GHz frequencies in the Industrial, Scientific, and Medical (ISM) band are open to the public and can be used without a license. As such, containing devices on another party’s network could have legal consequences.

The following example shows how to enable RLDP on all access points:

```
(Cisco Controller) > config rogue ap rldp enable alarm-only
```

The following example shows how to enable RLDP on monitor-mode access point ap_1:

```
(Cisco Controller) > config rogue ap rldp enable alarm-only ap_1
```

The following example shows how to start RLDP on the rogue access point with MAC address 123.456.789.000:

```
(Cisco Controller) > config rogue ap rldp initiate 123.456.789.000
```

The following example shows how to disable RLDP on all access points:

```
(Cisco Controller) > config rogue ap rldp disable
```

Related Commands

config rogue adhoc

config rogue ap classify

config rogue ap friendly

config rogue ap ssid

config rogue ap timeout

config rogue ap valid-client

config rogue client

config trapflags rogueap

show rogue ap clients

show rogue ap detailed

show rogue ap summary

show rogue ap friendly summary

show rogue ap malicious summary

show rogue ap unclassified summary

show rogue client detailed

show rogue client summary

show rogue ignore-list

show rogue rule detailed

show rogue rule summary

config rogue ap ssid

To generate an alarm only, or to automatically contain a rogue access point that is advertising your network's service set identifier (SSID), use the **config rogue ap ssid** command.

config rogue ap ssid {**alarm** | **auto-contain**}

Syntax Description

alarm	Generates only an alarm when a rogue access point is discovered to be advertising your network's SSID.
auto-contain	Automatically contains the rogue access point that is advertising your network's SSID.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

When you enter any of the containment commands, the following warning appears: "Using this feature may have legal consequences. Do you want to continue?" The 2.4- and 5-GHz frequencies in the Industrial, Scientific, and Medical (ISM) band are open to the public and can be used without a license. As such, containing devices on another party's network could have legal consequences.

The following example shows how to automatically contain a rogue access point that is advertising your network's SSID:

```
(Cisco Controller) > config rogue ap ssid auto-contain
```

Related Commands

config rogue adhoc

config rogue ap classify

config rogue ap friendly

config rogue ap rldp

config rogue ap timeout

config rogue ap valid-client

config rogue client

config trapflags rogueap

show rogue ap clients

show rogue ap detailed

show rogue ap summary

show rogue ap friendly summary

show rogue ap malicious summary

show rogue ap unclassified summary

show rogue client detailed

show rogue client summary

show rogue ignore-list

show rogue rule detailed

show rogue rule summary

config rogue ap timeout

To specify the number of seconds after which the rogue access point and client entries expire and are removed from the list, use the **config rogue ap timeout** command.

config rogue ap timeout *seconds*

Syntax Description

seconds	Value of 240 to 3600 seconds (inclusive), with a default value of 1200 seconds.

Command Default

The default number of seconds after which the rogue access point and client entries expire is 1200 seconds.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to set an expiration time for entries in the rogue access point and client list to 2400 seconds:

```
(Cisco Controller) > config rogue ap timeout 2400
```

Related Commands

config rogue ap classify

config rogue ap friendly

config rogue ap rldp

config rogue ap ssid

config rogue rule

config trapflags rogueap

show rogue ap clients

show rogue ap detailed

show rogue ap summary

show rogue ap friendly summary

show rogue ap malicious summary

show rogue ap unclassified summary

show rogue ignore-list

show rogue rule detailed

show rogue rule summary

config rogue auto-contain level

To configure rogue the auto-containment level, use the **config rogue auto-contain level** command.

config rogue auto-contain level *level* [**monitor_ap_only**]

Syntax Description

level	Rogue auto-containment level in the range of 1 to 4. You can enter a value of 0 to enable the Cisco WLC to automatically select the number of APs used for auto containment. The controller chooses the required number of APs based on the RSSI for effective containment. **Note** Up to four APs can be used to auto-contain when a rogue AP is moved to contained state through any of the auto-containment policies.
monitor_ap_only	(Optional) Configures auto-containment using only monitor AP mode.

Command Default

The default auto-containment level is 1.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

The controller continuously monitors all nearby access points and automatically discovers and collects information on rogue access points and clients. When the controller discovers a rogue access point, it uses any of the configured auto-containment policies to start autocontainment. The policies for initiating autocontainment are rogue on wire (detected through RLDP or rogue detector AP), rogue using managed SSID, Valid client on Rogue AP, and AdHoc Rogue.

This table lists the RSSI value associated with each containment level.

Table 1: RSSI Associated with Each Containment Level

Auto-containment Level	RSSI
1	0 to –55 dBm
2	–75 to –55 dBm
3	–85 to –75 dBm
4	Less than –85 dBm

Note RLDP is not supported for use with Cisco autonomous rogue access points. These access points drop the DHCP Discover request sent by the RLDP client. Also, RLDP is not supported if the rogue access point channel requires dynamic frequency selection (DFS).

When you enter any of the containment commands, the following warning appears:

```
Using this feature may have legal consequences. Do you want to continue? (y/n) :
```

The 2.4-GHz and 5-GHz frequencies in the Industrial, Scientific, and Medical (ISM) band are open to the public and can be used without a license. As such, containing devices on another party's network could have legal consequences.

The following example shows how to configure the auto-contain level to 3:

```
(Cisco Controller) > config rogue auto-contain level 3
```

Related Commands

config rogue adhoc

show rogue adhoc summary

show rogue client summary

show rogue ignore-list

show rogue rule summary

config rogue ap valid-client

To generate an alarm only, or to automatically contain a rogue access point to which a trusted client is associated, use the **config rogue ap valid-client** command.

config rogue ap valid-client {**alarm** | **auto-contain**}

Syntax Description

alarm	Generates only an alarm when a rogue access point is discovered to be associated with a valid client.
auto-contain	Automatically contains a rogue access point to which a trusted client is associated.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

When you enter any of the containment commands, the following warning appears: “Using this feature may have legal consequences. Do you want to continue?” The 2.4- and 5-GHz frequencies in the Industrial, Scientific, and Medical (ISM) band are open to the public and can be used without a license. As such, containing devices on another party’s network could have legal consequences.

The following example shows how to automatically contain a rogue access point that is associated with a valid client:

```
(Cisco Controller) > config rogue ap valid-client auto-contain
```

Related Commands

config rogue ap classify

config rogue ap friendly

config rogue ap rldp

config rogue ap timeout

config rogue ap ssid

config rogue rule

config trapflags rogueap

show rogue ap clients

show rogue ap detailed

show rogue ap summary

show rogue ap friendly summary

show rogue ap malicious summary

show rogue ap unclassified summary

show rogue ignore-list

show rogue rule detailed

show rogue rule summary

config rogue client

To configure rogue clients, use the **config rogue client** command.

config rogue client {**aaa** {**enable** | **disable**} | **alert** *ap_mac* | **contain** *client_mac* | **delete** {**state** {**alert** | **any** | **contained** | **contained-pending**} | **all** | **mac-address** *client_mac*} | **mse** {**enable** | **disable**} } }

Syntax Description

aaa	Configures AAA server or local database to validate whether rogue clients are valid clients. The default is disabled.
enable	Enables the AAA server or local database to check rogue client MAC addresses for validity.
disable	Disables the AAA server or local database to check rogue client MAC addresses for validity.
alert	Configures the controller to forward an immediate alert to the system administrator for further action.
ap_mac	Access point MAC address.
contain	Configures the controller to contain the offending device so that its signals no longer interfere with authorized clients.
client_mac	MAC address of the rogue client.
delete	Deletes the rogue client.
state	Deletes the rogue clients according to their state.
alert	Deletes the rogue clients in alert state.
any	Deletes the rogue clients in any state.
contained	Deletes all rogue clients that are in contained state.
contained-pending	Deletes all rogue clients that are in contained pending state.
all	Deletes all rogue clients.
mac-address	Deletes a rogue client with the configured MAC address.
mse	Validates if the rogue clients are valid clients using MSE. The default is disabled.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

You cannot validate rogue clients against MSE and AAA at the same time.

The following example shows how to enable the AAA server or local database to check MAC addresses:

```
(Cisco Controller) > config rogue client aaa enable
```

The following example shows how to disable the AAA server or local database from checking MAC addresses:

```
(Cisco Controller) > config rogue client aaa disable
```

Related Commands

config rogue rule

config trapflags rogueap

show rogue ap clients

show rogue ap detailed

show rogue client summary

show rogue ignore-list

show rogue rule detailed

show rogue rule summary

config rogue containment

To configure rogue containment, use the **config rogue containment** command.

config rogue containment {**flexconnect** | **auto-rate**} {**enable** | **disable**}

Syntax Description

flexconnect	Configures rogue containment for standalone FlexConnect APs.
auto-rate	Configures automatic rate selection for rogue containment.
enable	Enables the rogue containment.
disable	Disables the rogue containment.

Command Default

None

Command History

Release	Modification
7.5	This command was introduced.

Usage Guidelines

The following table lists the rogue containment automatic rate selection details.

Table 2: Rogue Containment Automatic Rate Selection

RSSI (dBm)	802.11b/g Tx Rate (Mbps)	802.11a Tx Rate (Mbps)
–74	1	6
–70	2	12
–55	5.5	12
< –40	5.5	18

The following example shows how to enable automatic rate selection for rogue containment:

```
(Cisco Controller) > config rogue containment auto-rate enable
```

config rogue detection

To enable or disable rogue detection, use the **config rogue detection** command.

Note If an AP itself is configured with the keyword **all**, the **all access points** case takes precedence over the AP that is with the keyword **all**.

config rogue detection {**enable** | **disable**} {*cisco_ap* | **all**}

Syntax Description

enable	Enables rogue detection on this access point.
disable	Disables rogue detection on this access point.
cisco_ap	Cisco access point.
all	Specifies all access points.

Command Default

The default rogue detection value is enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Rogue detection is enabled by default for all access points joined to the controller except for OfficeExtend access points. OfficeExtend access points are deployed in a home environment and are likely to detect a large number of rogue devices.

The following example shows how to enable rogue detection on the access point Cisco_AP:

```
(Cisco Controller) > config rogue detection enable Cisco_AP
```

Related Commands

config rogue rule

config trapflags rogueap

show rogue client detailed

show rogue client summary

show rogue ignore-list

show rogue rule detailed

show rogue rule summary

config rogue detection client-threshold

To configure the rogue client threshold for access points, use the **config rogue detection client-threshold** command.

config rogue detection client-threshold *value*

Syntax Description

value	Threshold rogue client count on an access point after which a trap is sent from the Cisco Wireless LAN Controller (WLC). The range is from 1 to 256. Enter 0 to disable the feature.

Command Default

The default rogue client threshold is 0.

Command History

Release	Modification
7.5	This command was introduced.

The following example shows how to configure the rogue client threshold:

```
(Cisco Controller) >config rogue detection client-threshold 200
```

config rogue detection min-rssi

To configure the minimum Received Signal Strength Indicator (RSSI) value at which APs can detect rogues and create a rogue entry in the controller, use the **config rogue detection min-rssi** command.

config rogue detection min-rssi *rssi-in-dBm*

Syntax Description

rssi-in-dBm	Minimum RSSI value. The valid range is from –70 dBm to –128 dBm, and the default value is –128 dBm.

Command Default

The default RSSI value to detect rogues in APs is -128 dBm.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

This feature is applicable to all the AP modes.

There can be many rogues with very weak RSSI values that do not provide any valuable information in rogue analysis. Therefore, you can use this option to filter rogues by specifying the minimum RSSI value at which APs should detect rogues.

The following example shows how to configure the minimum RSSI value:

```
(Cisco Controller) > config rogue detection min-rssi –80
```

Related Commands

config rogue detection

show rogue ap clients

config rogue rule

config trapflags rogueap

show rogue client detailed

show rogue client summary

show rogue ignore-list

show rogue rule detailed

show rogue rule summary

config rogue detection monitor-ap

To configure the rogue report interval for all monitor mode Cisco APs, use the **config rogue detection monitor-ap** command.

config rogue detection monitor-ap {**report-interval** | **transient-rogue-interval**} *time-in-seconds*

Syntax Description

report-interval	Specifies the interval at which rogue reports are sent.
transient-rogue-interval	Specifies the interval at which rogues are consistently scanned for by APs after the first time the rogues are scanned.
time-in-seconds	Time in seconds. The valid range is as follows: • 10 to 300 for **report-interval** • 120 to 1800 for **transient-rogue-interval**

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

This feature is applicable to APs that are in monitor mode only.

Using the transient interval values, you can control the time interval at which APs should scan for rogues. APs can also filter the rogues based on their transient interval values.

This feature has the following advantages:

- Rogue reports from APs to the controller are shorter.
- Transient rogue entries are avoided in the controller.
- Unnecessary memory allocation for transient rogues are avoided.

The following example shows how to configure the rogue report interval to 60 seconds:

```
(Cisco Controller) > config rogue detection monitor-ap report-interval 60
```

The following example shows how to configure the transient rogue interval to 300 seconds:

```
(Cisco Controller) > config rogue detection monitor-ap transient-rogue-interval 300
```

Related Commands

config rogue detection

config rogue detection min-rssi

config rogue rule

config trapflags rogueap

show rogue ap clients

show rogue client detailed

show rogue client summary

show rogue ignore-list

show rogue rule detailed

show rogue rule summary

config rogue detection report-interval

To configure the rogue detection report interval, use the **config rogue detection report-interval** command.

config rogue detection report-interval *time*

Syntax Description

time	Time interval, in seconds, at which the access points send the rogue detection report to the controller. The range is from 10 to 300.

Command Default

The default rogue detection report interval is 10 seconds.

Command History

Release	Modification
7.5	This command was introduced.

Usage Guidelines

This feature is applicable only to the access points that are in the monitor mode.

The following example shows how to configure the rogue detection report interval:

```
(Cisco Controller) >config rogue detection report-interval 60
```

config rogue detection security-level

To configure the rogue detection security level, use the **config rogue detection security-level** command.

config rogue detection security-level {**critical** | **custom** | **high** | **low**}

Syntax Description

critical	Configures the rogue detection security level to critical.
custom	Configures the rogue detection security level to custom, and allows you to configure the rogue policy parameters.
high	Configures the rogue detection security level to high. This security level configures basic rogue detection and auto containment for medium-scale or less critical deployments. The Rogue Location Discovery Protocol (RLDP) is disabled for this security level.
low	Configures the rogue detection security level to low. This security level configures basic rogue detection for small-scale deployments. Auto containment is not supported for this security level.

Command Default

The default rogue detection security level is custom.

Command History

Release	Modification
7.5	This command was introduced.

The following example shows how to configure the rogue detection security level to high:

```
(Cisco Controller) > config rogue detection security-level high
```

config rogue detection transient-rogue-interval

To configure the rogue-detection transient interval, use the **config rogue detection transient-rogue-interval** command.

config rogue detection transient-rogue-interval *time*

Syntax Description

time	Time interval, in seconds, at which a rogue should be consistently scanned by the access point after the rogue is scanned for the first time. The range is from 120 to 1800.

Command Default

The default rogue-detection transient interval for each security level is as follows:

- Low—120 seconds
- High—300 seconds
- Critical—600 seconds

Command History

Release	Modification
7.5	This command was introduced.

Usage Guidelines

This feature applies only to the access points that are in the monitor mode.

After the rogue is scanned consistently, updates are sent periodically to the Cisco Wireless LAN Controller (WLC). The access points filter the active transient rogues for a very short period and are then silent.

The following example shows how to configure the rogue detection transient interval:

```
(Cisco Controller) > config rogue detection transient-rogue-interval 200
```

config rogue rule

To add and configure rogue classification rules, use the **config rogue rule** command.

config rogue rule {**add ap priority** *priority* **classify** {**custom** *severity-score classification-name* | **friendly** | **malicious**} **notify** {**all** | **global** | **none** | **local**} **state** {**alert** | **contain** | **delete** | **internal** | **external**} *rule_name* | **classify** {**custom** *severity-score classification-name* | **friendly** | **malicious**} *rule_name* | **condition ap** {**set** | **delete**} *condition_type condition_value rule_name* | {**enable** | **delete** | **disable**} {**all** | *rule_name*} | **match** {**all** | **any**} | **priority** *priority* | **notify** {**all** | **global** | **none** | **local**} *rule_name* | **state** {**alert** | **contain** | **internal** | **external**} *rule_name*}

Syntax Description

add ap priority	Adds a rule with match any criteria and the priority that you specify.
priority	Priority of this rule within the list of rules.
classify	Specifies the classification of a rule.
custom	Classifies devices matching the rule as custom.
severity-score	Custom classification severity score of the rule. The range is from 1 to 100.
classification-name	Custom classification name. The name can be up to 32 case-sensitive, alphanumeric characters.
friendly	Classifies a rule as friendly.
malicious	Classifies a rule as malicious.
notify	Configures type of notification upon rule match.
all	Notifies the controller and a trap receiver such as Cisco Prime Infrastructure.
global	Notifies only a trap receiver such as Cisco Prime Infrastructure.
local	Notifies only the controller.
none	Notifies neither the controller nor a trap receiver such as Cisco Prime Infrastructure.
state	Configures state of the rogue access point after a rule match.
alert	Configures alert state on the rogue access point that is not in the neighbor list or in the user configured friendly MAC list. The controller forwards an immediate alert to the system administrator for further action.

contain	Configures contain state on the rogue access point. Controller contains the offending device so that its signals no longer interfere with authorized clients.
delete	Configures delete state on the rogue access point.
external	Configures external state on the rogue access point that is outside the network and poses no threat to WLAN security. The controller acknowledges the presence of this rogue access point.
internal	Configures alert state on rogue access point that is inside the network and poses no threat to WLAN security. The controller trusts this rogue access point.
rule_name	Rule to which the command applies, or the name of a new rule.
condition ap	Specifies the conditions for a rule that the rogue access point must meet.
set	Adds conditions to a rule that the rogue access point must meet.
delete	Removes conditions to a rule that the rogue access point must meet.
condition_type	Type of the condition to be configured. The condition types are listed below: • client-count—Requires that a minimum number of clients be associated to a rogue access point. The valid range is 1 to 10 (inclusive). • duration—Requires that a rogue access point be detected for a minimum period of time. The valid range is 0 to 3600 seconds (inclusive). • managed-ssid—Requires that a rogue access point's SSID be known to the controller. • no-encryption—Requires that a rogue access point's advertised WLAN does not have encryption enabled. • rssi—Requires that a rogue access point have a minimum RSSI value. The range is from –95 to –50 dBm (inclusive). • ssid—Requires that a rogue access point have a specific SSID. • substring-ssid—Requires that a rogue access point have a substring of a user-configured SSID.

condition_value	Value of the condition. This value is dependent upon the condition_type. For instance, if the condition type is ssid, then the condition value is either the SSID name or all.
enable	Enables all rules or a single specific rule.
delete	Deletes all rules or a single specific rule.
disable	Deletes all rules or a single specific rule.
match	Specifies whether a detected rogue access point must meet all or any of the conditions specified by the rule in order for the rule to be matched and the rogue access point to adopt the classification type of the rule.
all	Specifies all rules defined.
any	Specifies any rule meeting certain criteria.
priority	Changes the priority of a specific rule and shifts others in the list accordingly.

Command Default

No rogue rules are configured.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

For your changes to be effective, you must enable the rule. You can configure up to 64 rules.

Reclassification of rogue APs according to the RSSI condition of the rogue rule occurs only when the RSSI changes more than +/- 2 dBm of the configured RSSI value. Manual and automatic classification override custom rogue rules. Rules are applied to manually changed rogues if their class type changes to unclassified and state changes to alert. Adhoc rogues are classified and do not go to the pending state. You can have up to 50 classification types.

The following example shows how to create a rule called rule_1 with a priority of 1 and a classification as friendly.

```
(Cisco Controller) > config rogue rule add ap priority 1 classify friendly rule_1
```

The following example shows how to enable rule_1.

```
(Cisco Controller) > config rogue rule enable rule_1
```

The following example shows how to change the priority of the last command.

```
(Cisco Controller) > config rogue rule priority 2 rule_1
```

The following example shows how to change the classification of the last command.

```
(Cisco Controller) > config rogue rule classify malicious rule_1
```

The following example shows how to disable the last command.

```
(Cisco Controller) > config rogue rule disable rule_1
```

The following example shows how to delete SSID_2 from the user-configured SSID list in rule-5.

```
(Cisco Controller) > config rogue rule condition ap delete ssid ssid_2 rule-5
```

The following example shows how to create a custom rogue rule.

```
(Cisco Controller) > config rogue rule classify custom 1 VeryMalicious rule6
```

config rogue rule condition ap

To configure a condition of a rogue rule for rogue access points, use the **config rogue rule condition ap** command.

config rogue rule condition ap {**set** {**client-count** *count* | **duration** *time* | **managed-ssid** | **no-encryption** | **rssi** *rssi* | **ssid** *ssid* | **substring-ssid** *substring-ssid*} | **delete** {**all** | **client-count** | **duration** | **managed-ssid** | **no-encryption** | **rssi** | **ssid** | **substring-ssid**} *rule_name*

Syntax Description

set	Configures conditions to a rule that the rogue access point must meet.
client-count	Enables a minimum number of clients to be associated to the rogue access point.
count	Minimum number of clients to be associated to the rogue access point. The range is from 1 to 10 (inclusive). For example, if the number of clients associated to a rogue access point is greater than or equal to the configured value, the access point is classified as malicious.
duration	Enables a rogue access point to be detected for a minimum period of time.
time	Minimum time period, in seconds, to detect the rogue access point. The range is from 0 to 3600.
managed-ssid	Enables a rogue access point's SSID to be known to the controller.
no-encryption	Enables a rogue access point's advertised WLAN to not have encryption enabled. If a rogue access point has encryption disabled, it is likely that more clients will try to associate to it.
rssi	Enables a rogue access point to have a minimum Received Signal Strength Indicator (RSSI) value.
rssi	Minimum RSSI value, in dBm, required for the access point. The range is from –95 to –50 (inclusive). For example, if the rogue access point has an RSSI that is greater than the configured value, the access point is classified as malicious.
ssid	Enables a rogue access point have a specific SSID.
ssid	SSID of the rogue access point.
substring-ssid	Enables a rogue access point to have a substring of a user-configured SSID.
substring-ssid	Substring of a user-configured SSID. For example, if you have an SSID as ABCDE, you can specify the substring as ABCD or ABC. You can classify multiple SSIDs with matching patterns.
delete	Removes the conditions to a rule that a rogue access point must comply with.
all	Deletes all the rogue rule conditions.
rule_name	Rogue rule to which the command applies.

Command Default

The default value for RSSI is 0 dBm.

The default value for duration is 0 seconds.

The default value for client count is 0.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

You can configure up to 25 SSIDs per rogue rule. You can configure up to 25 SSID substrings per rogue rule.

The following example shows how to configure the RSSI rogue rule condition:

```
(Cisco Controller) > config rogue rule condition ap set rssi -50
```

config remote-lan session-timeout

To configure client session timeout, use the **config remote-lan session-timeout** command.

config remote-lan session-timeout *remote-lan-id seconds*

Syntax Description

remote-lan-id	Remote LAN identifier. Valid values are between 1 and 512.
seconds	Timeout or session duration in seconds. A value of zero is equivalent to no timeout.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the client session timeout to 6000 seconds for a remote LAN with ID 1:

```
(Cisco Controller) >config remote-lan session-timeout 1 6000
```

config rfid auto-timeout

To configure an automatic timeout of radio frequency identification (RFID) tags, use the **config rfid auto-timeout** command.

config rfid auto-timeout {**enable** | **disable**}

Syntax Description

enable	Enables an automatic timeout.
disable	Disables an automatic timeout.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable an automatic timeout of RFID tags:

```
(Cisco Controller) > config rfid auto-timeout enable
```

Related Commands

show rfid summary

config rfid status

config rfid timeout

config rfid status

To configure radio frequency identification (RFID) tag data tracking, use the **config rfid status** command.

config rfid status {**enable** | **disable**}

Syntax Description

enable	Enables RFID tag tracking.
disable	Enables RFID tag tracking.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure RFID tag tracking settings:

```
(Cisco Controller) > config rfid status enable
```

Related Commands

show rfid summary

config rfid auto-timeout

config rfid timeout

config rfid timeout

To configure a static radio frequency identification (RFID) tag data timeout, use the **config rfid timeout** command.

config rfid timeout *seconds*

Syntax Description

seconds	Timeout in seconds (from 60 to 7200).

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure a static RFID tag data timeout of 60 seconds:

```
(Cisco Controller) > config rfid timeout 60
```

Related Commands

show rfid summary

config rfid statistics

config rogue ap timeout

To specify the number of seconds after which the rogue access point and client entries expire and are removed from the list, use the **config rogue ap timeout** command.

config rogue ap timeout *seconds*

Syntax Description

seconds	Value of 240 to 3600 seconds (inclusive), with a default value of 1200 seconds.

Command Default

The default number of seconds after which the rogue access point and client entries expire is 1200 seconds.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to set an expiration time for entries in the rogue access point and client list to 2400 seconds:

```
(Cisco Controller) > config rogue ap timeout 2400
```

Related Commands

config rogue ap classify

config rogue ap friendly

config rogue ap rldp

config rogue ap ssid

config rogue rule

config trapflags rogueap

show rogue ap clients

show rogue ap detailed

show rogue ap summary

show rogue ap friendly summary

show rogue ap malicious summary

show rogue ap unclassified summary

show rogue ignore-list

show rogue rule detailed

show rogue rule summary

config route add

To configure a network route from the service port to a dedicated workstation IP address range, use the **config route add** command.

config route add *ip_address netmask gateway*

Syntax Description

ip_address	Network IP address.
netmask	Subnet mask for the network.
gateway	IP address of the gateway for the route network.

Command Default

None

Usage Guidelines

As on release 7.6, *IP_address* supports only IPv4 addresses.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6. This command supports only IPv4 address format.

The following example shows how to configure a network route to a dedicated workstation IP address 10.1.1.0, subnet mask 255.255.255.0, and gateway 10.1.1.1:

```
(Cisco Controller) > config route add 10.1.1.0 255.255.255.0 10.1.1.1
```

config route delete

To remove a network route from the service port, use the **config route delete** command.

config route delete *ip_address*

Syntax Description

ip_address	Network IP address.

Command Default

None

Usage Guidelines

As on release 7.6, *IP_address* supports only IPv4 addresses.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports only IPv6 address format.

The following example shows how to delete a route from the network IP address 10.1.1.0:

```
(Cisco Controller) > config route delete 10.1.1.0
```

config serial baudrate

To set the serial port baud rate, use the **config serial baudrate** command.

config serial baudrate {**1200** | **2400** | **4800** | **9600** | **19200** | **38400** | **57600**}

Syntax Description

1200	Specifies the supported connection speeds to 1200.
2400	Specifies the supported connection speeds to 2400.
4800	Specifies the supported connection speeds to 4800.
9600	Specifies the supported connection speeds to 9600.
19200	Specifies the supported connection speeds to 19200.
38400	Specifies the supported connection speeds to 38400.
57600	Specifies the supported connection speeds to 57600.

Command Default

The default serial port baud rate is 9600.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure a serial baud rate with the default connection speed of 9600:

```
(Cisco Controller) > config serial baudrate 9600
```

config serial timeout

To set the timeout of a serial port session, use the **config serial timeout** command.

config serial timeout *minutes*

Syntax Description

minutes	Timeout in minutes from 0 to 160. A value of 0 indicates no timeout.

Command Default

0 (no timeout)

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Use this command to set the timeout for a serial connection to the front of the Cisco wireless LAN controller from 0 to 160 minutes where 0 is no timeout.

The following example shows how to configure the timeout of a serial port session to 10 minutes:

```
(Cisco Controller) > config serial timeout 10
```

config service timestamps

To enable or disable time stamps in message logs, use the **config service timestamps** command.

config service timestamps {**debug** | **log**} {**datetime** | **disable**}

Syntax Description

debug	Configures time stamps in debug messages.
log	Configures time stamps in log messages.
datetime	Specifies to time-stamp message logs with the standard date and time.
disable	Specifies to prevent message logs being time-stamped.

Command Default

By default, the time stamps in message logs are disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure time-stamp message logs with the standard date and time:

```
(Cisco Controller) > config service timestamps log datetime
```

The following example shows how to prevent message logs being time-stamped:

```
(Cisco Controller) > config service timestamps debug disable
```

Related Commands

show logging

config sessions maxsessions

To configure the number of Telnet CLI sessions allowed by the Cisco wireless LAN controller, use the **config sessions maxsessions** command.

config sessions maxsessions *session_num*

Syntax Description

session_num	Number of sessions from 0 to 5.

Command Default

The default number of Telnet CLI sessions allowed by the Cisco WLC is 5.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Up to five sessions are possible while a setting of zero prohibits any Telnet CLI sessions.

The following example shows how to configure the number of allowed CLI sessions to 2:

```
(Cisco Controller) > config sessions maxsessions 2
```

Related Commands

show sessions

config sessions timeout

To configure the inactivity timeout for Telnet CLI sessions, use the **config sessions timeout** command.

config sessions timeout *timeout*

Syntax Description

timeout	Timeout of Telnet session in minutes (from 0 to 160). A value of 0 indicates no timeout.

Command Default

The default inactivity timeout for Telnet CLI sessions is 5 minutes.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the inactivity timeout for Telnet sessions to 20 minutes:

```
(Cisco Controller) > config sessions timeout 20
```

Related Commands

show sessions

config slot

To configure various slot parameters, use the **config slot** command.

config slot *slot_id* {**enable** | **disable** | **channel ap** | **chan_width** | **txpower ap** | **antenna extAntGain** *antenna_gain* | **rts**} *cisco_ap*

Syntax Description

slot_id	Slot downlink radio to which the channel is assigned. Beginning in Release 7.5 and later releases, you can configure 802.11a on slot 1 and 802.11ac on slot 2.
enable	Enables the slot.
disable	Disables the slot.
channel	Configures the channel for the slot.
ap	Configures one 802.11a Cisco access point.
chan_width	Configures channel width for the slot.
txpower	Configures Tx power for the slot.
antenna	Configures the 802.11a antenna.
extAntGain	Configures the 802.11a external antenna gain.
antenna_gain	External antenna gain value in .5 dBi units (such as 2.5 dBi = 5).
rts	Configures RTS/CTS for an access point.
cisco_ap	Name of the Cisco access point on which the channel is configured.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable slot 3 for the access point abc:

```
(Cisco Controller) >config slot 3 enable abc
```

The following example shows how to configure RTS for the access point abc:

```
(Cisco Controller) >config slot 2 rts abc
```

config switchconfig boot-break

To enable or disable the breaking into boot prompt by pressing the Esc key at system startup, use the **config switchconfig boot-break** command.

config switchconfig boot-break {**enable** | **disable**}

Syntax Description

enable	Enables the breaking into boot prompt by pressing the Esc key at system startup.
disable	Disables the breaking into boot prompt by pressing the Esc key at system startup.

Command Default

By default, the breaking into boot prompt by pressing the Esc key at system startup is disabled.

Usage Guidelines

You must enable the features that are prerequisites for the Federal Information Processing Standard (FIPS) mode before enabling or disabling the breaking into boot prompt.

The following example shows how to enable the breaking into boot prompt by pressing the Esc key at system startup:

```
(Cisco Controller) > config switchconfig boot-break enable
```

Related Commands

show switchconfig

config switchconfig flowcontrol

config switchconfig mode

config switchconfig secret-obfuscation

config switchconfig fips-prerequisite

config switchconfig strong-pwd

config switchconfig fips-prerequisite

To enable or disable the features that are prerequisites for the Federal Information Processing Standard (FIPS) mode, use the **config switchconfig fips-prerequisite** command.

config switchconfig fips-prerequisite {**enable** | **disable**}

Syntax Description

enable	Enables the features that are prerequisites for the FIPS mode.
disable	Disables the features that are prerequisites for the FIPS mode.

Command Default

By default, the features that are prerequisites for the FIPS mode are disabled.

Usage Guidelines

You must configure the FIPS authorization secret before you can enable or disable the FIPS prerequisite features.

The following example shows how to enable the features that are prerequisites for the FIPS mode:

```
(Cisco Controller) > config switchconfig fips-prerequisite enable
```

Related Commands

show switchconfig

config switchconfig flowcontrol

config switchconfig mode

config switchconfig secret-obfuscation

config switchconfig boot-break

config switchconfig strong-pwd

config switchconfig ucapl

To configure US Department of Defense (DoD) Unified Capabilities Approved Product List (APL) certification on the controller, use the **config switchconfig wlancc** command.

config switchconfig ucapl {**enable** | **disable**}

Syntax Description

enable	Enables UCAPL on the controller.
disable	Disables UCAPL on the controller.

Command Default

None

Command History

Release	Modification
8.0	This command was introduced.

The following example shows how to enable UCAPL on the controller:

```
(Cisco Controller) > config switchconfig ucapl enable
```

config switchconfig wlancc

To configure WLAN Common Criteria (CC) on the controller, use the **config switchconfig wlancc** command.

config switchconfig wlancc {**enable** | **disable**}

Syntax Description

enable	Enables WLAN CC on the controller.
disable	Disables WLAN CC on the controller.

Command Default

None

Command History

Release	Modification
8.0	This command was introduced.

The following example shows how to enable WLAN CC on the controller:

```
(Cisco Controller) > config switchconfig wlancc enable
```

config switchconfig strong-pwd

To enable or disable your controller to check the strength of newly created passwords, use the **config switchconfig strong-pwd** command.

config switchconfig strong-pwd {**case-check** | **consecutive-check** | **default-check** | **username-check** | **position-check** | **case-digit-check** | **minimum** {**upper-case** | **lower-case** | **digits** | **special-chars**} *no._of_characters* | **min-length** | *password_length* | **lockout**{**mgmtuser** | **snmpv3user** | **time** | **attempts**} | **lifetime** {**mgmtuser** | **snmpv3user**} *lifetime* | **all-checks**} {**enable** | **disable**}

Syntax Description

case-check	Checks at least three combinations: lowercase characters, uppercase characters, digits, or special characters.
consecutive-check	Checks the occurrence of the same character three times.
default-check	Checks for default values or use of their variants.
username-check	Checks whether the username is specified or not.
position-check	Checks whether the password has a four-character change from the old password.
case-digit-check	Checks whether the password has all the four combinations: lower, upper, digits, or special characters.
minimum	Checks whether the password has a minimum number of upper case and lower case characters, digits, or special characters.
upper-case	Checks whether the password has a minimum number of upper case characters.
lower-case	Checks whether the password has a minimum number of lower case characters.
digits	Checks whether the password has a minimum number of digits.
special-chars	Checks whether the password has a minimum number of special characters.
min-length	Configures the minimum length for the password.
password_length	Minimum length for the password. The range is from 3 to 24 case-sensitive characters.

lockout	Configures the lockout feature for a management user or Simple Network Management Protocol version 3 (SNMPv3) user.
mgmtuser	Locks out a management user when the number of successive failed attempts exceed the management user lockout attempts.
snmpv3user	Locks out a SNMPv3 user when the number of successive failed attempts exceeds the SNMPv3 user lockout attempts.
time	Configures the time duration after the lockout attempts when the management user or SNMPv3 user is locked.
attempts	Configures the number of successive incorrect password attempts after which the management user or SNMPv3 user is locked.
lifetime	Configures the number of days before the management user or SNMPv3 user requires a change of password due to the age of the password.
mgmtuser	Configures the number of days before the management user requires a change of password due to the password age.
snmpv3user	Configures the number of days before the SNMPv3 user requires a change of password due to the age of the password.
lifetime	Number of days before the management user or SNMPv3 user requir*lifetime*s a change of password due to the age of the password.
all-checks	Checks all the cases.
enable	Enables a strong password check for the access point and Cisco WLC.
disable	Disables a strong password check for the access point and Cisco WLC.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the Strong Password Check feature:

```
(Cisco Controller) > config switchconfig strong-pwd case-check enable
```

Related Commands

show switchconfig

config switchconfig flowcontrol

config switchconfig mode

config switchconfig secret-obfuscation

config switchconfig fips-prerequisite

config switchconfig boot-break

config switchconfig flowcontrol

To enable or disable 802.3x flow control, use the **config switchconfig flowcontrol** command.

config switchconfig flowcontrol {**enable** | **disable**}

Syntax Description

enable	Enables 802.3x flow control.
disable	Disables 802.3x flow control.

Command Default

By default, 802.3x flow control is disabled.

The following example shows how to enable 802.3x flow control on Cisco wireless LAN controller parameters:

```
(Cisco Controller) > config switchconfig flowcontrol enable
```

Related Commands

show switchconfig

config switchconfig mode

To configure Lightweight Access Port Protocol (LWAPP) transport mode for Layer 2 or Layer 3, use the **config switchconfig mode** command.

config switchconfig mode {**L2** | **L3**}

Syntax Description

L2	Specifies Layer 2 as the transport mode.
L3	Specifies Layer 3 as the transport mode.

Command Default

The default transport mode is L3.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure LWAPP transport mode to Layer 3:

```
(Cisco Controller) > config switchconfig mode L3
```

Related Commands

show switchconfig

config switchconfig secret-obfuscation

To enable or disable secret obfuscation, use the **config switchconfig secret-obfuscation** command.

config switchconfig secret-obfuscation {**enable** | **disable**}

Syntax Description

enable	Enables secret obfuscation.
disable	Disables secret obfuscation.

Command Default

Secrets and user passwords are obfuscated in the exported XML configuration file.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

To keep the secret contents of your configuration file secure, do not disable secret obfuscation. To further enhance the security of the configuration file, enable configuration file encryption.

The following example shows how to enable secret obfuscation:

```
(Cisco Controller) > config switchconfig secret-obfuscation enable
```

Related Commands

show switchconfig

config sysname

To set the Cisco wireless LAN controller system name, use the **config sysname** command.

config sysname *name*

Syntax Description

name	System name. The name can contain up to 24 alphanumeric characters.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the system named Ent_01:

```
(Cisco Controller) > config sysname Ent_01
```

Related Commands

show sysinfo

config snmp community accessmode

To modify the access mode (read only or read/write) of an SNMP community, use the **config snmp community accessmode** command.

config snmp community accessmode {**ro** | **rw**} *name*

Syntax Description

ro	Specifies a read-only mode.
rw	Specifies a read/write mode.
name	SNMP community name.

Command Default

Two communities are provided by default with the following settings:

```
SNMP Community Name Client IP Address Client IP Mask   Access Mode Status
------------------- ----------------- ---------------- ----------- ------
public              0.0.0.0           0.0.0.0          Read Only   Enable
private             0.0.0.0           0.0.0.0          Read/Write  Enable
```

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure read/write access mode for SNMP community:

```
(Cisco Controller) > config snmp community accessmode rw private
```

Related Commands

show snmp community

config snmp community mode

config snmp community create

config snmp community delete

config snmp community ipaddr

config snmp community create

To create a new SNMP community, use the **config snmp community create** command.

config snmp community create *name*

Syntax Description

name	SNMP community name of up to 16 characters.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Use this command to create a new community with the default configuration.

The following example shows how to create a new SNMP community named test:

```
(Cisco Controller) > config snmp community create test
```

Related Commands

show snmp community

config snmp community mode

config snmp community accessmode

config snmp community delete

config snmp community ipaddr

config snmp community delete

To delete an SNMP community, use the **config snmp community delete** command.

config snmp community delete *name*

Syntax Description

name	SNMP community name.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to delete an SNMP community named test:

```
(Cisco Controller) > config snmp community delete test
```

Related Commands

show snmp community

config snmp community mode

config snmp community accessmode

config snmp community create

config snmp community ipaddr

config snmp community ipaddr

To configure the IPv4 or IPv6 address of an SNMP community, use the **config snmp community ipaddr** command.

config snmp community ipaddr *IP addr IPv4 mask/IPv6 Prefix lengthname*

Syntax Description

IP addr	SNMP community IPv4 or IPv6 address.
IPv4 mask/IPv6 Prefix length	SNMP community IP mask (IPv4 mask or IPv6 Prefix length). The IPv6 prefix length is from 0 to 128.
name	SNMP community name.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports both IPv4 and IPv6 address formats.

Usage Guidelines

- This command is applicable for both IPv4 and IPv6 addresses.
- This command is not applicable for default SNMP community (public, private).

The following example shows how to configure an SNMP community with the IPv4 address 10.10.10.10, IPv4 mask 255.255.255.0, and SNMP community named comaccess:

```
(Cisco Controller) > config snmp community ipaddr 10.10.10.10 255.255.255.0 comaccess
```

The following example shows how to configure an SNMP community with the IPv6 address 2001:9:2:16::1, IPv6 prefix length 64, and SNMP community named comaccess:

```
(Cisco Controller) > config snmp community ipaddr 2001:9:2:16::1 64 comaccess
```

config snmp community mode

To enable or disable an SNMP community, use the **config snmp community mode** command.

config snmp community mode {**enable** | **disable**} *name*

Syntax Description

enable	Enables the community.
disable	Disables the community.
name	SNMP community name.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the SNMP community named public:

```
(Cisco Controller) > config snmp community mode disable public
```

Related Commands

show snmp community

config snmp community delete

config snmp community accessmode

config snmp community create

config snmp community ipaddr

config snmp engineID

To configure the SNMP engine ID, use the **config snmp engineID** command.

config snmp engineID {*engine_id* | **default**}

Syntax Description

engine_id	Engine ID in hexadecimal characters (a minimum of 10 and a maximum of 24 characters are allowed).
default	Restores the default engine ID.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

The SNMP engine ID is a unique string used to identify the device for administration purposes. You do need to specify an engine ID for the device because a default string is automatically generated using Cisco's enterprise number and the MAC address of the first interface on the device.

If you change the engine ID, then a reboot is required for the change to take effect.

Caution If you change the value of the SNMP engine ID, then the password of the user entered on the command line is converted to an MD5 (Message-Digest algorithm 5) or SHA (Secure Hash Algorithm) security digest. This digest is based on both the password and the local engine ID. The command line password is then deleted. Because of this deletion, if the local value of the engine ID changes, the security digests of the SNMP users will become invalid, and the users will have to be reconfigured.

The following example shows how to configure the SNMP engine ID with the value fffffffffff:

```
(Cisco Controller) > config snmp engineID fffffffffff
```

Related Commands

show snmpengineID

config snmp syscontact

To set the SNMP system contact name, use the **config snmp syscontact** command.

config snmp syscontact *contact*

Syntax Description

contact	SNMP system contact name. Valid value can be up to 255 printable characters.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to set the SMNP system contact named Cisco WLAN Solution_administrator:

```
(Cisco Controller) > config snmp syscontact Cisco WLAN Solution_administrator
```

config snmp syslocation

To configure the SNMP system location name, use the **config snmp syslocation** command.

config snmp syslocation *location*

Syntax Description

location	SNMP system location name. Valid value can be up to 255 printable characters.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the SNMP system location name to Building_2a:

```
(Cisco Controller) > config snmp syslocation Building_2a
```

config snmp trapreceiver create

To configure a server to receive SNMP traps, use the **config snmp trapreceiver create** command.

config snmp trapreceiver create *name IP addr*

Syntax Description

name	SNMP community name. The name contain up to 31 characters.
IP addr	Configure the IPv4 or IPv6 address of where to send SNMP traps.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports both IPv4 and IPv6 address formats.

Usage Guidelines

The IPv4 or IPv6 address must be valid for the command to add the new server.

The following example shows how to add a new SNMP trap receiver with the SNMP trap receiver named test and IP address 10.1.1.1:

```
(Cisco Controller) > config snmp trapreceiver create test 10.1.1.1
```

The following example shows how to add a new SNMP trap receiver with the SNMP trap receiver named test and IP address 2001:10:1:1::1:

```
(Cisco Controller) > config snmp trapreceiver create test 2001:10:1:1::1
```

config snmp trapreceiver delete

To delete a server from the trap receiver list, use the **config snmp trapreceiver delete** command.

config snmp trapreceiver delete *name*

Syntax Description

name	SNMP community name. The name can contain up to 16 characters.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to delete a server named test from the SNMP trap receiver list:

```
(Cisco Controller) > config snmp trapreceiver delete test
```

Related Commands

show snmp trap

config snmp trapreceiver mode

To send or disable sending traps to a selected server, use the **config snmp trapreceiver mode** command.

config snmp trapreceiver mode {**enable** | **disable**} *name*

Syntax Description

enable	Enables an SNMP trap receiver.
disable	Disables an SNMP trap receiver.
name	SNMP community name.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

This command enables or disables the Cisco wireless LAN controller from sending the traps to the selected server.

The following example shows how to disable an SNMP trap receiver from sending traps to a server named server1:

```
(Cisco Controller) > config snmp trapreceiver mode disable server1
```

Related Commands

show snmp trap

config snmp v3user create

To create a version 3 SNMP user, use the **config snmp v3user create** command.

config snmp v3user create *username* {**ro** | **rw**} {**none** | **hmacmd5** | **hmacsha**} {**none** | **des** | **aescfb128**} [*auth_key*] [*encrypt_key*]

Syntax Description

username	Version 3 SNMP username.
ro	Specifies a read-only user privilege.
rw	Specifies a read-write user privilege.
none	Specifies if no authentication is required.
hmacmd5	Specifies Hashed Message Authentication Coding Message Digest 5 (HMAC-MD5) for authentication.
hmacsha	Specifies Hashed Message Authentication Coding-Secure Hashing Algorithm (HMAC-SHA) for authentication.
none	Specifies if no encryption is required.
des	Specifies to use Cipher Block Chaining-Digital Encryption Standard (CBC-DES) encryption.
aescfb128	Specifies to use Cipher Feedback Mode-Advanced Encryption Standard-128 (CFB-AES-128) encryption.
auth_key	(Optional) Authentication key for the HMAC-MD5 or HMAC-SHA authentication protocol.
encrypt_key	(Optional) Encryption key for the CBC-DES or CFB-AES-128 encryption protocol.

Command Default

SNMP v3 username AccessMode Authentication Encryption

```
-------------------- ------------- -------------- -----------
default              Read/Write    HMAC-SHA       CFB-AES
```

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to add an SNMP username named test with read-only privileges and no encryption or authentication:

```
(Cisco Controller) > config snmp v3user create test ro none none
```

Related Commands **show snmpv3user**

config snmp v3user delete

To delete a version 3 SNMP user, use the **config snmp v3user delete** command.

config snmp v3user delete *username*

Syntax Description

username	Username to delete.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to remove an SNMP user named test:

```
(Cisco Controller) > config snmp v3user delete test
```

Related Commands

show snmp v3user

config snmp version

To enable or disable selected SNMP versions, use the **config snmp version** command.

config snmp version {**v1** | **v2** | **v3**} {**enable** | **disable**}

Syntax Description

v1	Specifies an SNMP version to enable or disable.
v2	Specifies an SNMP version to enable or disable.
v3	Specifies an SNMP version to enable or disable.
enable	Enables a specified version.
disable	Disables a specified version.

Command Default

By default, all the SNMP versions are enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable SNMP version v1:

```
(Cisco Controller) > config snmp version v1 enable
```

Related Commands

show snmpversion

config tacacs acct

To configure TACACS+ accounting server settings, use the **config tacacs acct** command.

config tacacs acct {**add***1-3 IP addr port ascii/hex secret* | **delete** *1-3* | **disable** *1-3* | **enable** *1-3* | **server-timeout** *1-3 seconds*}

Syntax Description

add	Adds a new TACACS+ accounting server.
1-3	Specifies TACACS+ accounting server index from 1 to 3.
IP addr	Specifies IPv4 or IPv6 address of the TACACS+ accounting server.
port	Specifies TACACS+ Server's TCP port.
ascii/hex	Specifies type of TACACS+ server's secret being used (ASCII or HEX).
secret	Specifies secret key in ASCII or hexadecimal characters.
delete	Deletes a TACACS+ server.
disable	Disables a TACACS+ server.
enable	Enables a TACACS+ server.
server-timeout	Changes the default server timeout for the TACACS+ server.
seconds	Specifies the number of seconds before the TACACS+ server times out. The server timeout range is from 5 to 30 seconds.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports both IPv4 and IPv6 address formats.

The following example shows how to add a new TACACS+ accounting server index 1 with the IPv4 address 10.0.0.0, port number 49, and secret key 12345678 in ASCII:

```
(Cisco Controller) > config tacacs acct add 1 10.0.0.0 10 ascii 12345678
```

The following example shows how to add a new TACACS+ accounting server index 1 with the IPv6 address 2001:9:6:40::623, port number 49, and secret key 12345678 in ASCII:

```
(Cisco Controller) > config tacacs acct add 1  2001:9:6:40::623 10 ascii 12345678
```

The following example shows how to configure the server timeout of 5 seconds for the TACACS+ accounting server:

```
(Cisco Controller) > config tacacs acct server-timeout 1 5
```

config tacacs auth

To configure TACACS+ authentication server settings, use the **config tacacs auth** command.

config tacacs auth { **add***1-3 IP addr port ascii/hex secret* | **delete** *1-3* | **disable** *1-3* | **enable** *1-3* | **mgmt-server-timeout** *1-3 seconds* | **server-timeout** *1-3seconds* }

Syntax Description

add	Adds a new TACACS+ accounting server.
1-3	TACACS+ accounting server index from 1 to 3.
IP addr	IP address for the TACACS+ accounting server.
port	Controller port used for the TACACS+ accounting server.
ascii/hex	Type of secret key being used (ASCII or HEX).
secret	Secret key in ASCII or hexadecimal characters.
delete	Deletes a TACACS+ server.
disable	Disables a TACACS+ server.
enable	Enables a TACACS+ server.
mgmt-server-timeout *1-3 seconds*	Changes the default management login server timeout for the server. The number of seconds before server times out is from 1 to 30 seconds.
server-timeout *1-3 seconds*	Changes the default network login server timeout for the server. The number of seconds before server times out is from 5 to 30 seconds.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports both IPv4 and IPv6 address formats.

The following example shows how to add a new TACACS+ authentication server index 1 with the IPv4 address 10.0.0.3, port number 49, and secret key 12345678 in ASCII:

```
(Cisco Controller) > config tacacs auth add 1 10.0.0.3 49 ascii 12345678
```

The following example shows how to add a new TACACS+ authentication server index 1 with the IPv6 address 2001:9:6:40::623, port number 49, and secret key 12345678 in ASCII:

```
(Cisco Controller) > config tacacs auth add 1 2001:9:6:40::623 49 ascii 12345678
```

The following example shows how to configure the server timeout for TACACS+ authentication server:

```
(Cisco Controller) > config tacacs auth server-timeout 1 5
```

config tacacs auth mgmt-server-timeout

To configure a default TACACS+ authentication server timeout for management users, use the **config tacacs auth mgmt-server-timeout** command.

config tacacs auth mgmt-server-timeout *index timeout*

Syntax Description

index	TACACS+ authentication server index.
timeout	Timeout value. The range is 1 to 30 seconds.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure a default TACACS+ authentication server timeout for management users:

```
(Cisco Controller) > config tacacs auth mgmt-server-timeout 1 10
```

Related Commands

config tacacs auth

config tacacs dns

To retrieve the TACACS IP information from a DNS server, use the **config radius dns** command.

config radius dns {**global** *port* {*ascii* | *hex*} *secret* | **query** *url timeout* | **serverip** *ip_address* | **disable** | **enable**}

Syntax Description

global	Configures the global port and secret to retrieve the TACACS IP information from a DNS server.
port	Port number for authentication. The range is from 1 to 65535. All the DNS servers should use the same authentication port.
ascii	Format of the shared secret that you should set to ASCII.
hex	Format of the shared secret that you should set to hexadecimal.
secret	TACACS server login secret.
query	Configures the fully qualified domain name (FQDN) of the TACACS server and DNS timeout.
url	FQDN of the TACACS server. The FQDN can be up to 63 case-sensitive, alphanumeric characters.
timeout	Maximum time that the Cisco Wireless LAN Controller (WLC) waits for, in days, before timing out a request and resending it. The range is from 1 to 180.
serverip	Configures the DNS server IP address.
ip_address	DNS server IP address.
disable	Disables the TACACS DNS feature. The default is disabled.
enable	Enables the Cisco WLC to retrieve the TACACS IP information from a DNS server.

Command Default

You cannot retrieve the TACACS IP information from a DNS server.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

The accounting port is derived from the authentication port. All the DNS servers should use the same secret. When you enable a DNS query, the static configurations will be overridden. The DNS list overrides the static AAA list.

The following example shows how to enable the TACACS DNS feature on the Cisco WLC:

```
(Cisco Controller) > config tacacs dns enable
```

config tacacs fallback-test interval

To configure TACACS+ probing interval, use the **config tacacs fallback-test interval** command.

config tacacs fallback-test interval { *seconds* }

Syntax Description

seconds	TACACS+ probing interval in seconds. Disable is 0, Range from 180 to 3600 seconds.

Command Default

None

Command History

Release	Modification
8.2	This command was introduced in this release.

The following example shows how to configure TACACS+ probing interval:

```
(Cisco Controller) >  config tacacs fallback-test interval 200
```

config time manual

To set the system time, use the **config time manual** command.

config time manual *MM* | *DD* | *YY HH* : *MM* : *SS*

Syntax Description

MM/*DD*/*YY*	Date.
HH:*MM*:*SS*	Time.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the system date to 04/04/2010 and time to 15:29:00:

```
(Cisco Controller) > config time manual 04/04/2010 15:29:00
```

Related Commands

show time

config time ntp

To set the Network Time Protocol (NTP), use the **config time ntp** command.

config time ntp {**auth** {**enable** *server-index key-index* | **disable** *server-index*} | **interval** *interval* | **key-auth** {**add** *key-index* **md5** {**ascii** | **hex**} *key*} | **delete** *key-index*} | **pollinterval** *maxpoll minpollserver-index* | **server** *index IP Address*}

Syntax Description

auth	Configures the NTP authentication.
enable	Enables the NTP authentication.
server-index	NTP server index.
key-index	Key index between 1 and 4294967295.
disable	Disables the NTP authentication.
interval	Configures the NTP version 3 polling interval.
interval	NTP polling interval in seconds. The range is from 3600 and 604800 seconds.
key-auth	Configures the NTP authentication key.
add	Adds an NTP authentication key.
md5	Specifies the authentication protocol.
ascii	Specifies the ASCII key type.
hex	Specifies the hexadecimal key type.
key	Specifies the ASCII key format with a maximum of 16 characters or the hexadecimal key format with a maximum of 32 digits.
delete	Deletes an NTP server.
pollinterval	Configures the Network Time Protocol version 4 Polling Interval.
maxpoll | *minpoll*	Enter maximum and minimum NTP polling interval in (power of 2) seconds.
server-index	Enter the NTP server index number.
server	Configures the NTP servers.
IP Address	NTP server's IP address. Use 0.0.0.0 or :: to delete entry.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Release	Modification
8.0	This command supports both IPv4 and IPv6 address formats.
8.6	This command was enhanced in this release. The new keywords added are pollinterval, maxpoll, minpoll.
8.6	The NTP server delete option is available with **config time ntp delete** *server-index*

Usage Guidelines

- To add the NTP server to the controller, use the **config time ntp server** *index IP Address* command.
- To display configured NTP server on the controller, use the **show time** command.

The following example shows how to configure the NTP polling interval to 7000 seconds:

```
(Cisco Controller) > config time ntp interval 7000
```

The following example shows how to enable NTP authentication where the server index is 4 and the key index is 1:

```
(Cisco Controller) > config time ntp auth enable 4 1
```

The following example shows how to add an NTP authentication key of value ff where the key format is in hexadecimal characters and the key index is 1:

```
(Cisco Controller) > config time ntp key-auth add 1 md5 hex ff
```

The following example shows how to add an NTP authentication key of value ff where the key format is in ASCII characters and the key index is 1:

```
(Cisco Controller) > config time ntp key-auth add 1 md5 ascii ciscokey
```

The following example shows how to add NTP servers and display the servers configured to controllers:

```
(Cisco Controller) > config time ntp server  1 10.92.125.52
(Cisco Controller) > config time ntp server  2 2001:9:6:40::623
(Cisco Controller) > show time
Time..................................... Fri May 23 12:04:18 2014

Timezone delta..................................... 0:0
Timezone location.............................. (GMT +5:30) Colombo, New Delhi, Chennai,
 Kolkata

NTP Servers
NTP Polling Interval........................ 3600

Index NTP Key Index  NTP Server NTP    Msg Auth Status
------- ------------------------------------------------
1            1      10.92.125.52       AUTH SUCCESS
2            1      2001:9:6:40::623   AUTH SUCCESS
```

The following example shows how to delete an NTP server:

```
(Cisco Controller) > config time ntp delete 1
```

config time ntp version

To configure the Network Time Protocol (NTP) version on the Cisco WLC, use the **config time ntp version** command.

Note During the NTP protocol version change, existing server(s) and keys on the Cisco WLC are deleted.

config time ntp version *version-number*

Syntax Description

version-number	Enter the NTP version 3 or 4 to run on the Cisco WLC.

Command Default

None

Command History

Release	Modification
8.6	This command was introduced.

The following example shows how to configure NTP version 4 on a Cisco WLC:

```
(Cisco Controller) > config time ntp version 4
```

config time timezone

To configure the system time zone, use the **config time timezone** command.

config time timezone {**enable** | **disable**} *delta_hours delta_mins*

Syntax Description

enable	Enables daylight saving time.
disable	Disables daylight saving time.
delta_hours	Local hour difference from the Universal Coordinated Time (UCT).
delta_mins	Local minute difference from UCT.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the daylight saving time:

```
(Cisco Controller) > config time timezone enable 2 0
```

Related Commands

show time

config time timezone location

To set the location of the time zone in order to have daylight saving time set automatically when it occurs, use the **config time timezone location** command.

config time timezone location *location_index*

Syntax Description

location_index	Number representing the time zone required. The time zones are as follows: • (GMT-12:00) International Date Line West • (GMT-11:00) Samoa • (GMT-10:00) Hawaii • (GMT-9:00) Alaska • (GMT-8:00) Pacific Time (US and Canada) • (GMT-7:00) Mountain Time (US and Canada) • (GMT-6:00) Central Time (US and Canada) • (GMT-5:00) Eastern Time (US and Canada) • (GMT-4:00) Atlantic Time (Canada) • (GMT-3:00) Buenos Aires (Argentina) • (GMT-2:00) Mid-Atlantic • (GMT-1:00) Azores • (GMT) London, Lisbon, Dublin, Edinburgh (default value) • (GMT +1:00) Amsterdam, Berlin, Rome, Vienna • (GMT +2:00) Jerusalem • (GMT +3:00) Baghdad • (GMT +4:00) Muscat, Abu Dhabi • (GMT +4:30) Kabul • (GMT +5:00) Karachi, Islamabad, Tashkent • (GMT +5:30) Colombo, Kolkata, Mumbai, New Delhi • (GMT +5:45) Katmandu • (GMT +6:00) Almaty, Novosibirsk • (GMT +6:30) Rangoon • (GMT +7:00) Saigon, Hanoi, Bangkok, Jakatar • (GMT +8:00) Hong Kong, Bejing, Chongquing • (GMT +9:00) Tokyo, Osaka, Sapporo • (GMT +9:30) Darwin • (GMT+10:00) Sydney, Melbourne, Canberra • (GMT+11:00) Magadan, Solomon Is., New Caledonia • (GMT+12:00) Kamchatka, Marshall Is., Fiji • (GMT+12:00) Auckland (New Zealand)

Command Default None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to set the location of the time zone in order to set the daylight saving time to location index 10 automatically:

```
(Cisco Controller) > config time timezone location 10
```

Related Commands **show time**

config trapflags 802.11-Security

To enable or disable sending 802.11 security-related traps, use the **config trapflags 802.11-Security** command.

config trapflags 802.11-Security wepDecryptError {**enable** | **disable**}

Syntax Description

enable	Enables sending 802.11 security-related traps.
disable	Disables sending 802.11 security-related traps.

Command Default

By default, sending the 802.11 security-related traps is enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to disable the 802.11 security related traps:

```
(Cisco Controller) > config trapflags 802.11-Security wepDecryptError disable
```

Related Commands

show trapflags

config trapflags aaa

To enable or disable the sending of AAA server-related traps, use the **config trapflags aaa** command.

config trapflags aaa {**auth** | **servers**} {**enable** | **disable**}

Syntax Description

auth	Enables trap sending when an AAA authentication failure occurs for management user, net user, or MAC filter.
servers	Enables trap sending when no RADIUS servers are responding.
enable	Enables the sending of AAA server-related traps.
disable	Disables the sending of AAA server-related traps.

Command Default

By default, the sending of AAA server-related traps is enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the sending of AAA server-related traps:

```
(Cisco Controller) > config trapflags aaa auth enable
```

Related Commands

show watchlist

config trapflags adjchannel-rogueap

To configure trap notifications when a rogue access point is detected at the adjacent channel, use the **config trapflags adjchannel-rogueap** command.

config trapflags adjchannel-rogueap {**enable** | **disable**}

Syntax Description

enable	Enables trap notifications when a rogue access point is detected at the adjacent channel.
disable	Disables trap notifications when a rogue access point is detected at the adjacent channel.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable trap notifications when a rogue access point is detected at the adjacent channel:

```
(Cisco Controller) > config trapflags adjchannel-rogueap enable
```

Related Commands

config trapflags 802.11-Security

config trapflags aaa

config trapflags ap

config trapflags authentication

config trapflags client

config trapflags configsave

config trapflags IPsec

config trapflags linkmode

config trapflags multiusers

config trapflags mesh

config trapflags strong-pwdcheck

config trapflags rfid

config trapflags rogueap

show trapflags

config trapflags ap

To enable or disable the sending of Cisco lightweight access point traps, use the **config trapflags ap** command.

config trapflags ap {**register** | **interfaceUp**} {**enable** | **disable**}

Syntax Description

register	Enables sending a trap when a Cisco lightweight access point registers with Cisco switch.
interfaceUp	Enables sending a trap when a Cisco lightweight access point interface (A or B) comes up.
enable	Enables sending access point-related traps.
disable	Disables sending access point-related traps.

Command Default

By default, the sending of Cisco lightweight access point traps is enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to prevent traps from sending access point-related traps:

```
(Cisco Controller) > config trapflags ap register disable
```

Related Commands

show trapflags

config trapflags authentication

To enable or disable sending traps with invalid SNMP access, use the **config trapflags authentication** command.

config trapflags authentication {**enable** | **disable**}

Syntax Description

enable	Enables sending traps with invalid SNMP access.
disable	Disables sending traps with invalid SNMP access.

Command Default

By default, the sending traps with invalid SNMP access is enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to prevent sending traps on invalid SNMP access:

```
(Cisco Controller) > config trapflags authentication disable
```

Related Commands

show trapflags

config trapflags client

To enable or disable the sending of client-related DOT11 traps, use the **config trapflags client** command.

config trapflags client {**802.11-associate 802.11-disassociate** | **802.11-deauthenticate** | **802.11-authfail** | **802.11-assocfail** | **authentication** | **excluded**} {**enable** | **disable**}

Syntax Description

802.11-associate	Enables the sending of Dot11 association traps to clients.
802.11-disassociate	Enables the sending of Dot11 disassociation traps to clients.
802.11-deauthenticate	Enables the sending of Dot11 deauthentication traps to clients.
802.11-authfail	Enables the sending of Dot11 authentication fail traps to clients.
802.11-assocfail	Enables the sending of Dot11 association fail traps to clients.
authentication	Enables the sending of authentication success traps to clients.
excluded	Enables the sending of excluded trap to clients.
enable	Enables sending of client-related DOT11 traps.
disable	Disables sending of client-related DOT11 traps.

Command Default

By default, the sending of client-related DOT11 traps is disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the sending of Dot11 disassociation trap to clients:

```
(Cisco Controller) > config trapflags client 802.11-disassociate enable
```

Related Commands

show trapflags

config trapflags client max-warning-threshold

To configure the threshold value of the number of clients that associate with the controller, after which an SNMP trap and a syslog message is sent to the controller, use the **config trapflags client max-warning-threshold** command.

config trapflags client max-warning-threshold {**threshold** | **enable** | **disable**}

Syntax Description

threshold	Configures the threshold percentage value of the number of clients that associate with the controller, after which an SNMP trap and a syslog message is sent to the controller. The range is from 80 to 100. The minimum interval between two warnings is 10 mins You cannot configure this interval.
enable	Enables the generation of the traps and syslog messages.
disable	Disables the generation of the traps and syslog messages.

Command Default

The default threshold value of the number of clients that associate with the controller is 90 %.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

This table lists the maximum number of clients for different controllers.

Table 3: Maximum Number of Clients Supported on Different Controllers

Controller	Maximum Number of Supported Clients
Cisco 5500 Series Controllers	7000
Cisco 2500 Series Controllers	500
Cisco Wireless Services Module 2	15000
Cisco Flex 7500 Series Controllers	64000
Cisco 8500 Series Controllers	64000
Cisco Virtual Wireless LAN Controllers	30000

The following example shows how to configure the threshold value of the number of clients that associate with the controller:

```
(Cisco Controller) > config trapflags client max-warning-threshold 80
```

Related Commands

show trapflags

config trapflags client

config trapflags configsave

To enable or disable the sending of configuration-saved traps, use the **config trapflags configsave** command.

config trapflags configsave {**enable** | **disable**}

Syntax Description

enable	Enables sending of configuration-saved traps.
disable	Disables the sending of configuration-saved traps.

Command Default

By default, the sending of configuration-saved traps is enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the sending of configuration-saved traps:

```
(Cisco Controller) > config trapflags configsave enable
```

Related Commands

show trapflags

config trapflags IPsec

To enable or disable the sending of IPsec traps, use the **config trapflags IPsec** command.

config trapflags IPsec {**esp-auth** | **esp-reply** | **invalidSPI** | **ike-neg** | **suite-neg** | **invalid-cookie**} {**enable** | **disable**}

Syntax Description

esp-auth	Enables the sending of IPsec traps when an ESP authentication failure occurs.
esp-reply	Enables the sending of IPsec traps when an ESP replay failure occurs.
invalidSPI	Enables the sending of IPsec traps when an ESP invalid SPI is detected.
ike-neg	Enables the sending of IPsec traps when an IKE negotiation failure occurs.
suite-neg	Enables the sending of IPsec traps when a suite negotiation failure occurs.
invalid-cookie	Enables the sending of IPsec traps when a Isakamp invalid cookie is detected.
enable	Enables sending of IPsec traps.
disable	Disables sending of IPsec traps.

Command Default

By default, the sending of IPsec traps is enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the sending of IPsec traps when ESP authentication failure occurs:

```
(Cisco Controller) > config trapflags IPsec esp-auth enable
```

Related Commands

show trapflags

config trapflags linkmode

To enable or disable Cisco wireless LAN controller level link up/down trap flags, use the **config trapflags linkmode** command.

config trapflags linkmode {**enable** | **disable**}

Syntax Description

enable	Enables Cisco wireless LAN controller level link up/down trap flags.
disable	Disables Cisco wireless LAN controller level link up/down trap flags.

Command Default

By default, the Cisco WLC level link up/down trap flags are enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the Cisco wireless LAN controller level link up/down trap:

```
(Cisco Controller) > config trapflags linkmode disable
```

Related Commands

show trapflags

config trapflags mesh

To configure trap notifications when a mesh access point is detected, use the **config trapflags mesh** command.

config trapflags mesh {**enable** | **disable**}

Syntax Description

enable	Enables trap notifications when a mesh access point is detected.
disable	Disables trap notifications when a mesh access point is detected.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable trap notifications when a mesh access point is detected:

```
(Cisco Controller) > config trapflags mesh enable
```

Related Commands

config trapflags 802.11-Security

config trapflags aaa

config trapflags ap

config trapflags adjchannel-rogueap

config trapflags authentication

config trapflags client

config trapflags configsave

config trapflags IPsec

config trapflags linkmode

config trapflags multiusers

config trapflags strong-pwdcheck

config trapflags rfid

config trapflags rogueap

show trapflags

config trapflags multiusers

To enable or disable the sending of traps when multiple logins are active, use the **config trapflags multiusers** command.

config trapflags multiusers {**enable** | **disable**}

Syntax Description

enable	Enables the sending of traps when multiple logins are active.
disable	Disables the sending of traps when multiple logins are active.

Command Default

By default, the sending of traps when multiple logins are active is enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to disable the sending of traps when multiple logins are active:

```
(Cisco Controller) > config trapflags multiusers disable
```

Related Commands

show trapflags

config trapflags rfid

To configure the threshold value of the maximum number of radio frequency identification (RFID) tags, after which an SNMP trap and a syslog message is sent to the controller, use the **config trapflags rfid** command.

config trapflags rfid {**threshold** | **enable** | **disable**}

Syntax Description

threshold	Configures the threshold percentage value of the maximum number of RFID tags, after which an SNMP trap and a syslog message is sent to the controller. The range is from 80 to 100. The traps and syslog messages are generated every 10 minutes. You cannot configure this interval.
enable	Enables the generation of the traps and syslog messages.
disable	Disables the generation of the traps and syslog messages.

Command Default

The default threshold value of the maximum number of RFID tags is 90 %.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

The following table shows the maximum number of RFID tags supported on different controllers:

Table 4: Maximum Number of RFID Tags Supported on Different Controllers

Controller	Maximum Number of Supported Clients
Cisco 5500 Series Controllers	5000
Cisco 2500 Series Controllers	500
Cisco Wireless Services Module 2	10000
Cisco Flex 7500 Series Controllers	50000
Cisco 8500 Series Controllers	50000
Cisco Virtual Wireless LAN Controllers	3000

The following example shows how to configure the threshold value of the maximum number of RFID tags:

```
(Cisco Controller) > config trapflags rfid 80
```

Related Commands

config trapflags 802.11-Security

config trapflags aaa

config trapflags ap

config trapflags adjchannel-rogueap

config trapflags authentication

config trapflags client

config trapflags configsave

config trapflags IPsec

config trapflags linkmode

config trapflags multiusers

config trapflags mesh

config trapflags strong-pwdcheck

config trapflags rogueap

config trapflags mesh

show trapflags

config trapflags rogueap

To enable or disable sending rogue access point detection traps, use the **config trapflags rogueap** command.

config trapflags rogueap {**enable** | **disable**}

Syntax Description

enable	Enables the sending of rogue access point detection traps.
disable	Disables the sending of rogue access point detection traps.

Command Default

By default, the sending of rogue access point detection traps is enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to disable the sending of rogue access point detection traps:

```
(Cisco Controller) > config trapflags rogueap disable
```

Related Commands

config rogue ap classify

config rogue ap friendly

config rogue ap rldp

config rogue ap ssid

config rogue ap timeout

config rogue ap valid-client

show rogue ap clients

show rogue ap detailed

show rogue ap summary

show rogue ap friendly summary

show rogue ap malicious summary

show rogue ap unclassified summary

show trapflags

config trapflags rrm-params

To enable or disable the sending of Radio Resource Management (RRM) parameters traps, use the **config trapflags rrm-params** command.

config trapflags rrm-params {**tx-power** | **channel** | **antenna**} {**enable** | **disable**}

Syntax Description

tx-power	Enables trap sending when the RF manager automatically changes the tx-power level for the Cisco lightweight access point interface.
channel	Enables trap sending when the RF manager automatically changes the channel for the Cisco lightweight access point interface.
antenna	Enables trap sending when the RF manager automatically changes the antenna for the Cisco lightweight access point interface.
enable	Enables the sending of RRM parameter-related traps.
disable	Disables the sending of RRM parameter-related traps.

Command Default

By default, the sending of RRM parameters traps is enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the sending of RRM parameter-related traps:

```
(Cisco Controller) > config trapflags rrm-params tx-power enable
```

Related Commands

show trapflags

config trapflags rrm-profile

To enable or disable the sending of Radio Resource Management (RRM) profile-related traps, use the **config trapflags rrm-profile** command.

config trapflags rrm-profile {**load** | **noise** | **interference** | **coverage**} {**enable** | **disable**}

Syntax Description

load	Enables trap sending when the load profile maintained by the RF manager fails.
noise	Enables trap sending when the noise profile maintained by the RF manager fails.
interference	Enables trap sending when the interference profile maintained by the RF manager fails.
coverage	Enables trap sending when the coverage profile maintained by the RF manager fails.
enable	Enables the sending of RRM profile-related traps.
disable	Disables the sending of RRM profile-related traps.

Command Default

By default, the sending of RRM profile-related traps is enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to disable the sending of RRM profile-related traps:

```
(Cisco Controller) > config trapflags rrm-profile load disable
```

Related Commands

show trapflags

config trapflags stpmode

To enable or disable the sending of spanning tree traps, use the **config trapflags stpmode** command.

config trapflags stpmode {**enable** | **disable**}

Syntax Description

enable	Enables the sending of spanning tree traps.
disable	Disables the sending of spanning tree traps.

Command Default

By default, the sending of spanning tree traps is enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to disable the sending of spanning tree traps:

```
(Cisco Controller) > config trapflags stpmode disable
```

Related Commands

show trapflags

config trapflags strong-pwdcheck

To configure trap notifications for strong password checks, use the **config trapflags strong-pwdcheck** command.

config trapflags strong-pwdcheck {**enable** | **disable**}

Syntax Description

enable	Enables trap notifications for strong password checks.
disable	Disables trap notifications for strong password checks.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable trap notifications for strong password checks:

```
(Cisco Controller) > config trapflags strong-pwdcheck enable
```

Related Commands

config trapflags 802.11-Security

config trapflags aaa

config trapflags ap

config trapflags adjchannel-rogueap

config trapflags authentication

config trapflags client

config trapflags configsave

config trapflags IPsec

config trapflags linkmode

config trapflags multiusers

config trapflags mesh

config trapflags rfid

config trapflags rogueap

show trapflags

config trapflags wps

To enable or disable Wireless Protection System (WPS) trap sending, use the **config trapflags wps** command.

config trapflags wps {**enable** | **disable**}

Syntax Description

enable	Enables WPS trap sending.
disable	Disables WPS trap sending.

Command Default

By default, the WPS trap sending is enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to disable the WPS traps sending:

```
(Cisco Controller) > config trapflags wps disable
```

Related Commands

show trapflags

config tunnel eogre heart-beat

To configure the keep alive ping interval duration, use the **config tunnel eogre** command.

config tunnel eogre heart-beat {**interval** | **max-skip-count**} *number-value*

Syntax Description

interval *number-value*	Time interval between echo request message in seconds.
max-skip-count *number-value*	Maximum number of retries before the member is considered non functional.

Command Default

The default value of heart-beat *interval* is 60 seconds. Range is between 10 to 600 seconds.

The default value of heart-beat *max-skip-count* is 3 retries. Range is between 3 to 10 retries.

Command History

Release	Modification
8.1	This command was introduced.

The following example shows how to set the heart-beat interval value '45 seconds' :

```
config tunnel eogre heart-beat interval 45
```

config tunnel eogre gateway

To configure the Ethernet over GRE gateway IPv4 address, use the **config tunnel eogre gateway** command.

config tunnel eogre gateway { { { **add** | **modify** } *gateway-name* { **ipv4-address** | **ipv6-address** } *gateway-ip-address* } | { **delete** *gateway-name* } }

Syntax Description

add	Adds new gateway.
delete	Removes a gateway.
modify	Modifies an existing gateway.
ipv4-address	To enter the IPv4 address of the gateway.
ipv6-address	To enter the IPv6 address of the gateway.
gateway-ip-address	IPv4 or IPv6 address of the gateway.
gateway-name	Tunnel gateway name.

Command Default

None

Command History

Release	Modification
8.1	This command was introduced.
8.3	The IPv6 address format option for the tunnel gateway was added.

- IPv4 address example

```
config tunnel eogre gateway add hurricane ipv4 192.168.10.1
```

- IPv6 address example

```
config tunnel eogre gateway add hurricane ipv6 2001:DB8::1
```

config tunnel eogre domain

To perform tunnel gateway domain configuration, use the **config tunnel eogre domain** command.

config tunnel eogre domain { { **create** | **delete** } *domain-name* } { **add** | **remove** } *domain-name gateway-name*

Syntax Description

create	Creates new gateway domain name.
delete	Deletes gateway domain.
add	Add gateway name to domain
remove	Remove gateway name from domain
domain-name	Domain name
gateway-name	Gateway name

Command Default

None

Command History

Release	Modification
8.1	This command was introduced.

The following example shows how to create new gateway domain name:

```
config tunnel eogre domain create web.com data
```

config tunnel eogre domain primary

To add primary or secondary gateway name to a domain, use the **config tunnel eogre domain primary** command.

config tunnel eogre domain primary *domain-name gateway-name*

Syntax Description

domain-name	Enter the domain name
gateway-name	Enter the gateway name to be added to the domain

Usage Guidelines

In a domain, the primary gateway is active by default. When the primary gateway is not operational, the secondary gateway becomes the active gateway. Clients will have to associate again with the secondary gateway. During and after failover, Cisco WLC continues to ping the primary gateway. When the primary gateway is operational again, the primary gateway becomes the active gateway. Clients then fall back to the primary gateway. The same option is available for the TGW from FlexConnect in local switched mode. EoGRE tunnels can be DTLS encrypted CAPWAP IPv4 or IPv6. This feature is supported on all Wave 1 and Wave 2 APs that are supported in this release.

Command History

Release	Modification
8.5	This command was introduced.

config tunnel profile

To create, copy, or delete a profile, use the **config tunnel profile** command.

config tunnel profile {**copy** | **create** | **delete**} *profile-name*

Syntax Description

copy	Copies an existing profile.
create	Creates a new profile.
delete	Deletes an existing profile.

Command Default

None

Command History

Release	Modification
8.1	This command was introduced.

The following example shows how to create a profile:

```
config tunnel profile create floorone
```

config tunnel profile_rule

To add or modify a rule in a profile, use the **config tunnel profile** command.

config tunnel profile rule {**add** | **modify** }*profile-name* **realm-filter** *realm-string* **eogre vlan** *vlan-id gateway-domain-name*

Syntax Description

add	Adds a new rule.
modify	Modifies an existing rule.

Command Default

None

Command History

Release	Modification
8.1	This command was introduced.

The following example shows how to add a rule to a profile:

```
config tunnel profile add table realm filter 5 eogre vlan 3 web.com
```

config tunnel profile_rule-delete

To delete a rule from a profile, use the **config tunnel profile** command.

config tunnel profile ruledelete *profile-name* **realm-filter** *realm-string*

Syntax Description

delete	Deletes an existing rule from a profile.

Command Default

None

Command History

Release	Modification
8.1	This command was introduced.

The following example shows how to delete a rule from a profile:

```
config tunnel profile delete table realm filter 5
```

config tunnel profile eogre-DHCP82

To enable or disable the DHCP option 82 parameter, use the **config tunnel profile** command.

config tunnel profile eogre *profile-name* **DHCP-Opt-82** {**enable** | **disable**}

Syntax Description

enable	Enables DHCP option 82 parameter in the system.
disable	Disables DHCP option 82 parameter in the system.

Command Default

None

Command History

Release	Modification
8.1	This command was introduced.

The following example shows how to enable the DHCP option 82 parameter:

```
config tunnel profile eogre test dhcp-opt-82 enable
```

config tunnel profile eogre-gateway-radius-proxy

To enable or disable the gateway-radius-proxy, use the **config tunnel profile** command.

config tunnel profile eogre *profile-name* **gateway-radius-proxy** {**enable** | **disable**}

Syntax Description

enable	Enables Gateway as Radius Proxy.
disable	Disables Gateway as Radius Proxy.

Command Default

None

Command History

Release	Modification
8.1	This command was introduced.

The following example shows how to enable the gateway proxy:

```
config tunnel profile eogre test gateway-radius-proxy enable
```

config tunnel profile eogre-gateway-radius-proxy-accounting

To enable or disable the gateway as accounting radius-proxy, use the **config tunnel profile** command.

config tunnel profile eogre *profile-name* **gateway-radius-proxy accounting** {**enable** | **disable**}

Syntax Description

enable	Enables Gateway as accounting Radius Proxy.
disable	Disables Gateway as accounting Radius Proxy.

Command Default

None

Command History

Release	Modification
8.1	This command was introduced.

The following example shows how to disable the gateway as accounting radius proxy:

```
config tunnel profile eogre test gateway-radius-proxy accounting disable
```

config tunnel profile eogre-DHCP82

To enable or disable the DHCP option 82 parameter, use the **config tunnel profile** command.

config tunnel profile eogre *profile-name* **DHCP-Opt-82** {**enable** | **disable**}

Syntax Description

enable	Enables DHCP option 82 parameter in the system.
disable	Disables DHCP option 82 parameter in the system.

Command Default

None

Command History

Release	Modification
8.1	This command was introduced.

The following example shows how to enable the DHCP option 82 parameter:

```
config tunnel profile eogre test dhcp-opt-82 enable
```

config tunnel profile eogre-DHCP82-circuit-id

To set format for circuit-id field in DHCP option 82 parameter, use the **config tunnel profile** command.

config tunnel profile eogre *profile-name* **DHCP-Opt-82 circuit-id** *parameter-id*

Syntax Description

circuit-id	Sets the format for the Circuit-ID field in DHCP option 82
parameter-id	List of supported parameters: • ap-mac • ap-ethmac • ap-name • ap-group-name • flex-group-name • ap-location • vlan-id • SSID-name • SSID-TYPE • Client-mac

Command Default

None

Command History

Release	Modification
8.1	This command was introduced.

The following example shows how to set the format for circuit-id in the DHCP option 82 parameter:

```
config tunnel profile eogre test dhcp-opt-82 circuit-id access1bldg
```

config tunnel profile eogre-DHCP82-delimiter

To set the delimiter for the DHCP option 82 parameter, use the **config tunnel profile** command.

config tunnel profile eogre *profile-name* **DHCP-Opt-82 delimiter** *delimiter character*

Syntax Description

delimiter	Sets the delimiter for the DHCP option 82 parameter in the system.
delimiter character	Delimiter is used to separate the DHCP option 82 parameter.

Command Default

None

Command History

Release	Modification
8.1	This command was introduced.

The following example shows how to delimit the DHCP option 82 parameter:

```
config tunnel profile eogre test dhcp-opt-82 delimiter -
```

config tunnel profile eogre-DHCP82-format

To set the required format for DCHP option 82, use the **config tunnel profile** command.

config tunnel profile eogre *profile-name* **dhcp-opt-82 format** {**binary** | **ascii**}

Syntax Description

binary	Set Format for DHCP option 82 as Binary
ascii	Set Format for DHCP option 82 as Ascii

Command Default

None

Command History

Release	Modification
8.1	This command was introduced.

The following example shows how to set 'binary' format to the DHCP option 82 parameter:

```
config tunnel profile eogre test dhcp-opt-82 format binary
```

config tunnel profile eogre-DHCP82-remote-id

To set format for remote-id field in DHC P option 82 parameter, use the **config tunnel profile** command.

config tunnel profile eogre *profile-name* **DHCP-Opt-82 remote-id** *parameter-id*

Syntax Description

remote-id	Sets the format for the Remote-ID field in DHCP option 82
parameter-id	List of supported parameters: • ap-mac • ap-ethmac • ap-name • ap-group-name • flex-group-name • ap-location • vlan-id • SSID-name • SSID-TYPE • Client-mac

Command Default

None

Command History

Release	Modification
8.1	This command was introduced.

The following example shows how to set the format for remote-id in the DHCP option 82 parameter:

```
config tunnel profile eogre test dhcp-opt-82 remote-id access1flr
```

config watchlist add

To add a watchlist entry for a wireless LAN, use the **config watchlist add** command.

config watchlist add {**mac** *MAC* | **username** *username*}

Syntax Description

mac *MAC*	Specifies the MAC address of the wireless LAN.
username *username*	Specifies the name of the user to watch.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to add a watchlist entry for the MAC address a5:6b:ac:10:01:6b:

```
(Cisco Controller) >config watchlist add mac a5:6b:ac:10:01:6b
```

config watchlist delete

To delete a watchlist entry for a wireless LAN, use the **config watchlist delete** command.

config watchlist delete {**mac** *MAC* | **username** *username*}

Syntax Description

mac *MAC*	Specifies the MAC address of the wireless LAN to delete from the list.
username *username*	Specifies the name of the user to delete from the list.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to delete a watchlist entry for the MAC address a5:6b:ac:10:01:6b:

```
(Cisco Controller) >config watchlist delete mac a5:6b:ac:10:01:6b
```

config watchlist disable

To disable the client watchlist, use the **config watchlist disable** command.

config watchlist disable

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to disable the client watchlist:

```
(Cisco Controller) >config watchlist disable
```

config watchlist enable

To enable a watchlist entry for a wireless LAN, use the **config watchlist enable** command.

config watchlist enable

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable a watchlist entry:

```
(Cisco Controller) >config watchlist enable
```

config wgb vlan

To configure the Workgroup Bridge (WGB) VLAN client support, use the **config wgb vlan** command.

config wgb vlan {**enable** | **disable**}

Syntax Description

enable	Enables wired clients behind a WGB to connect to an anchor controller in a Data Management Zone (DMZ).
disable	Disables wired clients behind a WGB from connecting to an anchor controller in a DMZ.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable WGB VLAN client support:

```
(Cisco Controller) >config wgb vlan enable
```

config wlan

To create, delete, enable, or disable a wireless LAN, use the **config wlan** command.

config wlan {**enable** | **disable** | **create** | **delete**} *wlan_id* [*name* | **foreignAp** *name ssid* | **all**]

Syntax Description

enable	Enables a wireless LAN.
disable	Disables a wireless LAN.
create	Creates a wireless LAN.
delete	Deletes a wireless LAN.
wlan_id	Wireless LAN identifier between 1 and 512.
name	(Optional) WLAN profile name up to 32 alphanumeric characters.
foreignAp	(Optional) Specifies the third-party access point settings.
ssid	SSID (network name) up to 32 alphanumeric characters.
all	(Optional) Specifies all wireless LANs.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

When you create a new WLAN using the **config wlan create** command, it is created in disabled mode. Leave it disabled until you have finished configuring it.

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 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.

The following example shows how to enable wireless LAN identifier 16:

```
(Cisco Controller) >config wlan enable 16
```

config wlan 7920-support

To configure support for phones, use the **config wlan 7920-support** command.

config wlan 7920-support {**client-cac-limit** | **ap-cac-limit**} {**enable** | **disable**} *wlan_id*

Syntax Description

ap-cac-limit	Supports phones that require client-controlled Call Admission Control (CAC) that expect the Cisco vendor-specific information element (IE).
client-cac-limit	Supports phones that require access point-controlled CAC that expect the IEEE 802.11e Draft 6 QBSS-load.
enable	Enables phone support.
disable	Disables phone support.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

You cannot enable both WMM mode and client-controlled CAC mode on the same WLAN.

The following example shows how to enable the phone support that requires client-controlled CAC with wireless LAN ID 8:

```
(Cisco Controller) >config wlan 7920-support ap-cac-limit enable 8
```

config wlan 802.11e

To configure 802.11e support on a wireless LAN, use the **config wlan 802.11e** command.

config wlan 802.11e {**allow** | **disable** | **require**} *wlan_id*

Syntax Description

allow	Allows 802.11e-enabled clients on the wireless LAN.
disable	Disables 802.11e on the wireless LAN.
require	Requires 802.11e-enabled clients on the wireless LAN.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

802.11e provides quality of service (QoS) support for LAN applications, which are critical for delay sensitive applications such as Voice over Wireless IP (VoWIP).

802.11e enhances the 802.11 Media Access Control layer (MAC layer) with a coordinated time division multiple access (TDMA) construct, and adds error-correcting mechanisms for delay sensitive applications such as voice and video. The 802.11e specification provides seamless interoperability and is especially well suited for use in networks that include a multimedia capability.

The following example shows how to allow 802.11e on the wireless LAN with LAN ID 1:

```
(Cisco Controller) >config wlan 802.11e allow 1
```

config wlan aaa-override

To configure a user policy override via AAA on a wireless LAN, use the **config wlan aaa-override** command.

config wlan aaa-override {**enable** | **disable**} {*wlan_id* | **foreignAp**}

Syntax Description

enable	Enables a policy override.
disable	Disables a policy override.
wlan_id	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.

Command Default

AAA is disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

When AAA override is enabled and a client has conflicting AAA and Cisco wireless LAN controller wireless LAN authentication parameters, client authentication is performed by the AAA server. As part of this authentication, the operating system will move clients from the default Cisco wireless LAN VLAN to a VLAN returned by the AAA server and predefined in the controller interface configuration (only when configured for MAC filtering, 802.1X, and/or WPA operation). In all cases, the operating system will also use QoS, DSCP, 802.1p priority tag values, and ACLs provided by the AAA server, as long as they are predefined in the controller interface configuration. (This VLAN switching by AAA override is also referred to as Identity Networking.)

If the corporate wireless LAN uses a management interface assigned to VLAN 2, and if AAA override returns a redirect to VLAN 100, the operating system redirects all client transmissions to VLAN 100, regardless of the physical port to which VLAN 100 is assigned.

When AAA override is disabled, all client authentication defaults to the controller authentication parameter settings, and authentication is performed by the AAA server if the controller wireless LAN does not contain any client-specific authentication parameters.

The AAA override values might come from a RADIUS server.

The following example shows how to configure user policy override via AAA on WLAN ID 1:

```
(Cisco Controller) >config wlan aaa-override enable 1
```

config wlan acl

To configure a wireless LAN access control list (ACL), use the **config wlan acl** command.

config wlan acl [*acl_name* | **none**]

Syntax Description

wlan_id	Wireless LAN identifier (1 to 512).
acl_name	(Optional) ACL name.
none	(Optional) Clears the ACL settings for the specified wireless LAN.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure a WLAN access control list with WLAN ID 1 and ACL named office_1:

```
(Cisco Controller) >config wlan acl 1 office_1
```

config wlan apgroup

To manage access point group VLAN features, use the **config wlan apgroup** command.

config wlan apgroup {**add** *apgroup_name* [*description*] | **delete** *apgroup_name* | **description** *apgroup_name description* | **interface-mapping** {**add** | **delete**} *apgroup_name wlan_id interface_name* | **nac-snmp** {**enable** | **disable**} *apgroup_name wlan_id* | **nasid** *NAS-ID apgroup_name* | **profile-mapping** {**add** | **delete**} *apgroup_name profile_name* | **wlan-radio-policy** *apgroup_name wlan-id* {**802.11a-only** | **802.11bg** | **802.11g-only** | **all**} | **hotspot** {**venue** {**type** *apgroup_name group_codetype_code* | **name** *apgroup_name language_codevenue_name* } | **operating-class** {**add** | **delete**} *apgroup_name operating_class_value*} }

Syntax Description

add	Creates a new access point group (AP group).
apgroup_name	Access point group name.
wlan_id	Wireless LAN identifier from 1 to 512.
delete	Removes a wireless LAN from an AP group.
description	Describes an AP group.
description	Description of the AP group.
interface-mapping	(Optional) Assigns or removes a Wireless LAN
interface_name	(Optional) Interface to which you want to map
nac-snmp	Configures NAC SNMP functionality on given disables Network Admission Control (NAC) ou access point group.
enable	Enables NAC out-of-band support on an AP gr
disable	Disables NAC out-of-band support on an AP g
NAS-ID	Network Access Server identifier (NAS-ID) for is sent to the RADIUS server by the controller (the authentication request, which is used to classi You can enter up to 32 alphanumeric characters and later releases, you can configure the NAS-I or an access point group. The order of priority i WLAN NAS-ID > Interface NAS-ID.
none	Configures the controller system name as the N
profile-mapping	Configures RF profile mapping on an AP group
profile_name	RF profile name for a specified AP group.
wlan-radio-policy	Configures WLAN radio policy on an AP grou

802.11a-only	Configures WLAN radio policy on an AP group.
802.11bg	Configures WLAN radio policy on an AP group.
802.11g-only	Configures WLAN radio policy on an AP group.
all	Configures WLAN radio policy on an AP group.
hotspot	Configures a HotSpot on an AP group.
venue	Configures venue information for an AP group.
type	Configures the type of venue for an AP group.
group_code	Venue group information for an AP group. The following options are available: • 0 : UNSPECIFIED • 1 : ASSEMBLY • 2 : BUSINESS • 3 : EDUCATIONAL • 4 : FACTORY-INDUSTRIAL • 5 : INSTITUTIONAL • 6 : MERCANTILE • 7 : RESIDENTIAL • 8 : STORAGE • 9 : UTILITY-MISC • 10 : VEHICULAR • 11 : OUTDOOR

type_code

Venue type information for an AP group.

For venue group 1 (ASSEMBLY), the following op

- 0 : UNSPECIFIED ASSEMBLY
- 1 : ARENA
- 2 : STADIUM
- 3 : PASSENGER TERMINAL
- 4 : AMPHITHEATER
- 5 : AMUSEMENT PARK
- 6 : PLACE OF WORSHIP
- 7 : CONVENTION CENTER
- 8 : LIBRARY
- 9 : MUSEUM
- 10 : RESTAURANT
- 11 : THEATER
- 12 : BAR
- 13 : COFFEE SHOP
- 14 : ZOO OR AQUARIUM
- 15 : EMERGENCY COORDINATION CENT

For venue group 2 (BUSINESS), the following opt

- 0 : UNSPECIFIED BUSINESS
- 1 : DOCTOR OR DENTIST OFFICE
- 2 : BANK
- 3 : FIRE STATION
- 4 : POLICE STATION
- 6 : POST OFFICE
- 7 : PROFESSIONAL OFFICE
- 8 : RESEARCH AND DEVELOPMENT FAC
- 9 : ATTORNEY OFFICE

For venue group 3 (EDUCATIONAL), the followin

- 0 : UNSPECIFIED EDUCATIONAL
- 1 : PRIMARY SCHOOL
- 2 : SECONDARY SCHOOL

- 3 : UNIVERSITY OR COLLEGE

For venue group 4 (FACTORY-INDUSTRIAL) available:

- 0 : UNSPECIFIED FACTORY AND IND
- 1 : FACTORY

For venue group 5 (INSTITUTIONAL), the follo

- 0 : UNSPECIFIED INSTITUTIONAL
- 1 : HOSPITAL
- 2 : LONG-TERM CARE FACILITY
- 3 : ALCOHOL AND DRUG RE-HABILI
- 4 :GROUP HOME
- 5 :PRISON OR JAIL

For venue group 6 (MERCANTILE), the follov

- 0 : UNSPECIFIED MERCANTILE
- 1 : RETAIL STORE
- 2 : GROCERY MARKET
- 3 : AUTOMOTIVE SERVICE STATION
- 4 : SHOPPING MALL
- 5 : GAS STATION

For venue group 7 (RESIDENTIAL), the follov

- 0 : UNSPECIFIED RESIDENTIAL
- 1 : PRIVATE RESIDENCE
- 2 : HOTEL OR MOTEL
- 3 : DORMITORY
- 4 : BOARDING HOUSE

For venue group 8 (STORAGE), the following

- 0 : UNSPECIFIED STORAGE

For venue group 9 (UTILITY-MISC), the follo

- 0 : UNSPECIFIED UTILITY AND MISC

For venue group 10 (VEHICULAR), the following

- 0 : UNSPECIFIED VEHICULAR
- 1 : AUTOMOBILE OR TRUCK
- 2 : AIRPLANE
- 3 : BUS
- 4 : FERRY
- 5 : SHIP OR BOAT
- 6 : TRAIN
- 7 : MOTOR BIKE

For venue group 11 (OUTDOOR), the following o

- 0 : UNSPECIFIED OUTDOOR
- 1 : MINI-MESH NETWORK
- 2 : CITY PARK
- 3 : REST AREA
- 4 : TRAFFIC CONTROL
- 5 : BUS STOP
- 6 : KIOSK

name	Configures the name of venue for an AP group.
language_code	An ISO-639 encoded string defining the language string is a three character language code. For exam for English.
venue_name	Venue name for this AP group. This name is associ service set (BSS) and is used in cases where the SS enough information about the venue. The venue nar can be up to 252 alphanumeric characters.
add	Adds an operating class for an AP group.
delete	Deletes an operating class for an AP group.
operating_class_value	Operating class for an AP group. The available ope 83, 84, 112, 113, 115, 116, 117, 118, 119, 120, 121 126, 127.

Command Default

AP Group VLAN is disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

An error message appears if you try to delete an access point group that is used by at least one access point. Before you can delete an AP group in controller software release 6.0, move all APs in this group to another group. The access points are not moved to the default-group access point group as in previous releases. To see the APs, enter the **show wlan apgroups** command. To move APs, enter the **config ap group-name** *groupname cisco_ap* command.

The NAS-ID configured on the controller for AP group or WLAN or interface is used for authentication. The NAS-ID is not propagated across controllers.

The following example shows how to enable the NAC out-of band support on access point group 4:

```
(Cisco Controller) >config wlan apgroup nac enable apgroup 4
```

config wlan apgroup atf 802.11

Configure Cisco Airtime Fairness at an AP group level by using the **config wlan apgroup atf 802.11** command.

config wlan apgroups atf 802.11 {**a** | **b**} {**mode** {**disable** | **monitor** | **enforce-policy**} *ap-group-name*} | {**optimization** {**enable** | **disable**}}

Syntax Description

a	Specifies the 802.11a network settings
b	Specifies the 802.11b/g network settings
mode	Configures the granularity of Cisco ATF enforcement
disable	Disables Cisco ATF
monitor	Configures Cisco ATF in monitor mode
enforce-policy	Configures Cisco ATF in enforcement mode
ap-group-name	AP group name that you must specify
optimization	Configures airtime optimization
enable	Enables airtime optimization
disable	Disabled airtime optimization

Command History

Release	Modification
8.1	This command was introduced

To configure Cisco ATF in enforcement mode on an 802.11a network, for an AP group *my-ap-group*, enter the following command:

```
(Cisco Controller) >config wlan apgroup atf 802.11a mode enforce-policy my-ap-group
```

config wlan apgroup atf 802.11 policy

To configure AP group-level override for Cisco ATF policy on a WLAN by using this command:

config wlan apgroup atf 802.11 {**a** | **b**} **policy** *ap-group-name wlan-id policy-name* **override** {**enable** | **disable**}

Syntax Description

a	Specifies the 802.11a network settings
b	Specifies the 802.11b network settings
policy	Specifies the Cisco ATF policy
ap-group-name	Name of the AP group that you must specify
wlan-id	WLAN ID or Remote LAN ID that you must specify
policy-name	Cisco ATF policy name that you must specify
override	Configures ATF policy override for a WLAN in the AP group
enable	Enables ATF policy override for a WLAN in the AP group
disable	Disables ATF policy override for a WLAN in the AP group

Command History

Release	Modification
8.1	This command was introduced

config wlan apgroup opendns-profile

To configure an open Domain Name System (DNS) profile to an access point (AP) group wireless LAN (WLAN), use the **config wlan apgroup opendns-profile** command.

config wlan apgroup opendns-profile*wlan-id site-name profile-name* **enable**

Syntax Description

wlan-id	WLAN identifier.
site-name	Name of the AP group to configure.
profile-name	OpenDNS profile name used for tracking this profile.
enable	Enables OpenDNS identity.
disable	Disables OpenDNS identity.

Command Default

The OpenDNS profile for an AP group WLAN is not created.

Command Modes

(Controller Configuration) >

Command History

Release	Modification
8.4	This command was introduced.

Usage Guidelines

None

Example

The following example shows how to configure an openDNS profile to an AP group WLAN:

```
(Cisco Controller) > config wlan apgroup opendns-profile wlan1 site1 user1
```

config wlan apgroup qinq

To configure 802.1Q-in-Q VLAN tagging of traffic for an AP group, use the **config wlan apgroup qinq** command.

config wlan apgroup qinq {**tagging** {**client-traffic | dhcp-v4 | eap-sim-aka**} *apgroup_name* {**enable | disable**} | **service-vlan** *apgroup_name vlan_id*}

Syntax Description

tagging	Configures 802.1Q-in-Q VLAN tagging of traffic.
client-traffic	Configures 802.1Q-in-Q tagging of client traffic for an AP group.
dhcp-v4	Configures 802.1Q-in-Q tagging of DHCPv4 traffic for an AP group.
eap-sim-aka	Configures 802.1Q-in-Q tagging of Extensible Authentication Protocol for Authentication and Key Agreement (EAP-AKA) and EAP for Global System for Mobile Communications Subscriber Identity Module (EAP-SIM) traffic for an AP group.
enable	Enables 802.1Q-in-Q tagging of traffic.
disable	Disables 802.1Q-in-Q tagging of traffic.
service-vlan	Configures service VLAN for an AP group.
apgroup_name	Name of the access point group.
vlan_id	VLAN identifier.

Command Default

By default, 802.1Q-in-Q tagging of client and DHCPv4 traffic for an AP group is disabled.

Command History

Release	Modification
8.0	This command was introduced.

Usage Guidelines

Note You must enable 802.1Q-in-Q tagging of client traffic before you enable 802.1Q-in-Q tagging of DHCPv4 traffic.

When you enable 802.1Q-in-Q tagging of client traffic, the 802.1Q-in-Q tagging of EAP-AKA and EAP-SIM traffic is also enabled.

The following example shows how to enable 802.1Q-in-Q tagging of client traffic for an AP group:

```
(Cisco Controller) >config wlan apgroup qinq tagging client-traffic APg1 enable
```

The following example shows how to configure the service VLAN for an AP group:

```
(Cisco Controller) >config wlan apgroup qinq service-vlan APg1 10
```

config wlan assisted-roaming

To configure assisted roaming on a WLAN, use the **config wlan assisted-roaming** command.

config wlan assisted-roaming {**neighbor-list** | **dual-list** | **prediction**} {**enable** | **disable**} *wlan_id*

Syntax Description

neighbor-list	Configures an 802.11k neighbor list for a WLAN.
dual-list	Configures a dual band 802.11k neighbor list for a WLAN. The default is the band that the client is currently associated with.
prediction	Configures an assisted roaming optimization prediction for a WLAN.
enable	Enables the configuration on the WLAN.
disable	Disables the configuration on the WLAN.
wlan_id	Wireless LAN identifier between 1 and 512 (inclusive).

Command Default

The 802.11k neighbor list is enabled for all WLANs.

By default, dual band list is enabled if the neighbor list feature is enabled for the WLAN.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

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.

The following example shows how to enable an 802.11k neighbor list for a WLAN:

```
(Cisco Controller) >config wlan assisted-roaming neighbor-list enable 1
```

config wlan atf

Map a WLAN to a Cisco ATF policy using the **config wlan atf** command.

config wlan atf *wlan-id* **policy** *policy-id*

Syntax Description

wlan-id	WLAN ID that you must specify to which the Cisco ATF policy has to be mapped.
policy	Specifies the Cisco ATF policy
policy-id	Cisco ATF policy ID that you must specify

Command History

Release	Modification
8.1	This command was introduced

config wlan avc

To configure Application Visibility and Control (AVC) on a WLAN, use the **config wlan avc** command.

config wlan avc *wlan_id* {**profile** *profile_name* | **visibility**} {**enable** | **disable**}

Syntax Description

wlan_id	Wireless LAN identifier from 1 to 512.
profile	Associates or removes an AVC profile from a WLAN.
profile_name	Name of the AVC profile. The profile name can be up to 32 case-sensitive, alphanumeric characters.
visibility	Configures application visibility on a WLAN.
enable	Enables application visibility on a WLAN. You can view the classification of applications based on the Network Based Application Recognition (NBAR) deep packet inspection technology. Use the **show avc statistics client** command to view the client AVC statistics.
disable	Disables application visibility on a WLAN.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

You can configure only one AVC profile per WLAN and each AVC profile can have up to 32 rules. Each rule states a Mark or Drop action for an application, which allows you to configure up to 32 application actions per WLAN. You can configure up to 16 AVC profiles on a controller and associate an AVC profile with multiple WLANs.

The following example shows how to associate an AVC profile with a WLAN:

```
(Cisco Controller) >config wlan avc 5 profile profile1 enable
```

config wlan band-select allow

To configure band selection on a WLAN, use the **config wlan band-select allow** command.

config wlan band-select allow {**enable** | **disable**} *wlan_id*

Syntax Description

enable	Enables band selection on a WLAN.
disable	Disables band selection on a WLAN.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

When you enable band select on a WLAN, the access point suppresses client probes on 2.4-GHz 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. Band selection can be used only with Cisco Aironet 1040, 1140, and 1250 Series and the 3500 series access points.

The following example shows how to enable band selection on a WLAN:

```
(Cisco Controller) >config wlan band-select allow enable 6
```

config wlan broadcast-ssid

To configure an Service Set Identifier (SSID) broadcast on a wireless LAN, use the **config wlan broadcast-ssid** command.

config wlan broadcast-ssid {**enable** | **disable**} *wlan_id*

Syntax Description

enable	Enables SSID broadcasts on a wireless LAN.
disable	Disables SSID broadcasts on a wireless LAN.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

Broadcasting of SSID is disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure an SSID broadcast on wireless LAN ID 1:

```
(Cisco Controller) >config wlan broadcast-ssid enable 1
```

config wlan call-snoop

To enable or disable Voice-over-IP (VoIP) snooping for a particular WLAN, use the **config wlan call-snoop** command.

config wlan call-snoop {**enable** | **disable**} *wlan_id*

Syntax Description

enable	Enables VoIP snooping on a wireless LAN.
disable	Disables VoIP snooping on a wireless LAN.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

WLAN should be with Platinum QoS and it needs to be disabled while invoking this CLI

The following example shows how to enable VoIP snooping for WLAN 3:

```
(Cisco Controller) >config wlan call-snoop 3 enable
```

config wlan chd

To enable or disable Coverage Hole Detection (CHD) for a wireless LAN, use the **config wlan chd** command.

config wlan chd *wlan_id* {**enable** | **disable**}

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.
enable	Enables SSID broadcasts on a wireless LAN.
disable	Disables SSID broadcasts on a wireless LAN.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable CHD for WLAN 3:

```
(Cisco Controller) >config wlan chd 3 enable
```

config wlan ccx aironet-ie

To enable or disable Aironet information elements (IEs) for a WLAN, use the **config wlan ccx aironet-ie** command.

config wlan ccx aironet-ie {**enable** | **disable**}

Syntax Description

enable	Enables the Aironet information elements.
disable	Disables the Aironet information elements.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable Aironet information elements for a WLAN:

```
(Cisco Controller) >config wlan ccx aironet-ie enable
```

config wlan channel-scan defer-priority

To configure the controller to defer priority markings for packets that can defer off channel scanning, use the **config wlan channel-scan defer-priority** command.

config wlan channel-scan defer-priority *priority* [**enable** | **disable**] *wlan_id*

Syntax Description

priority	User priority value (0 to 7).
enable	(Optional) Enables packet at given priority to defer off channel scanning.
disable	(Optional) Disables packet at gven priority to defer off channel scanning.
wlan_id	Wireless LAN identifier (1 to 512).

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

The priority value should be set to 6 on the client and on the WLAN.

The following example shows how to enable the controller to defer priority markings that can defer off channel scanning with user priority value 6 and WLAN id 30:

```
(Cisco Controller) >config wlan channel-scan defer-priority 6 enable 30
```

config wlan channel-scan defer-time

To assign the channel scan defer time in milliseconds, use the **config wlan channel-scan defer-time** command.

config wlan channel-scan defer-time *msecs wlan_id*

Syntax Description

msecs	Deferral time in milliseconds (0 to 60000 milliseconds).
wlan_id	Wireless LAN identifier from 1 to 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

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

The following example shows how to assign the scan defer time to 40 milliseconds for WLAN with ID 50:

```
(Cisco Controller) >config wlan channel-scan defer-time 40 50
```

config wlan custom-web

To configure the web authentication page for a WLAN, use the **config wlan custom-web** command.

config wlan custom-web { {**ext-webauth-url** *ext-webauth-url wlan_id* } | {**global** {**enable** | **disable**} } | {**ms-open** {**enable** | **disable** | **url**} } | {**login-page** *page-name* } | {**loginfailure-page** {*page-name* | **none**} } | {**logout-page** {*page-name* | **none**} } | {**sleep-client** {**enable** | **disable**} *wlan_id* **timeout** *duration*} | {**webauth-type** {**internal** | **customized** | **external**} *wlan_id*} }

Syntax Description

ext-webauth-url	Configures an external web authentication URL.
ext-webauth-url	External web authentication URL.
wlan_id	WLAN identifier. Default range is from 1 to 512.
global	Configures the global status for a WLAN.
enable	Enables the global status for a WLAN.
disable	Disables the global status for a WLAN.
ms-open	Configures the ms-open feature on the WLAN.
enable	Enables the ms-open feature on the WLAN.
disable	Disables the ms-open feature on the WLAN.
url	Configures ms-open URL.
login-page	Configures the name of the login page for an external web authentication URL.
page-name	Login page name for an external web authentication URL.
loginfailure-page	Configures the name of the login failure page for an external web authentication URL.
none	Does not configure a login failure page for an external web authentication URL.
logout-page	Configures the name of the logout page for an external web authentication URL.
sleep-client	Configures the sleep client feature on the WLAN.
timeout	Configures the sleep client timeout on the WLAN.
duration	Maximum amount of time after the idle timeout, in hours, before a sleeping client is forced to reauthenticate. The range is from 1 to 720. The default is 12. When the sleep client feature is enabled, the clients need not provide the login credentials when they move from one Cisco WLC to another (if the Cisco WLCs are in the same mobility group) between the sleep and wake-up times.
webauth-type	Configures the type of web authentication for the WLAN.
internal	Displays the default login page.

customized	Displays a customized login page.
external	Displays a login page on an external web server.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.2	This command was modified and the ms-open parameters were added.

The following example shows how to configure web authentication type in the WLAN.

```
Cisco Controller config wlan custom-web webauth-type external
```

config wlan dhcp_server

To configure the internal DHCP server for a wireless LAN, use the **config wlan dhcp_server** command.

config wlan dhcp_server {*wlan_id* | **foreignAp**} *ip_address* [**required**]

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.
ip_address	IP address of the internal DHCP server (this parameter is required).
required	(Optional) Specifies whether DHCP address assignment is required.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

The preferred method for configuring DHCP is to use the primary DHCP address assigned to a particular interface instead of the DHCP server override. If you enable the override, you can use the **show wlan** command to verify that the DHCP server has been assigned to the WLAN.

The following example shows how to configure an IP address 10.10.2.1 of the internal DHCP server for wireless LAN ID 16:

```
(Cisco Controller) >config wlan dhcp_server 16 10.10.2.1
```

config wlan diag-channel

To enable the diagnostic channel troubleshooting on a particular WLAN, use the **config wlan diag-channel** command.

config wlan diag-channel [**enable** | **disable**] *wlan_id*

Syntax Description

enable	(Optional) Enables the wireless LAN diagnostic channel.
disable	(Optional) Disables the wireless LAN diagnostic channel.
wlan_id	Wireless LAN identifier (1 to 512).

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the wireless LAN diagnostic channel for WLAN ID 1:

```
(Cisco Controller) >config wlan diag-channel enable 1
```

config wlan dtim

To configure a Delivery Traffic Indicator Message (DTIM) for 802.11 radio network **config wlan dtim** command.

config wlan dtim {**802.11a** | **802.11b**} *dtim wlan_id*

Syntax Description

802.11a	Configures DTIM for the 802.11a radio network.
802.11b	Configures DTIM for the 802.11b radio network.
dtim	Value for DTIM (between 1 to 255 inclusive).
wlan_id	Number of the WLAN to be configured.

Command Default

The default is DTIM 1.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure DTIM for 802.11a radio network with DTIM value 128 and WLAN ID 1:

```
(Cisco Controller) >config wlan dtim 802.11a 128 1
```

config wlan exclusionlist

To configure the wireless LAN exclusion list, use the **config wlan exclusionlist** command.

config wlan exclusionlist {*wlan_id* [**enabled** | **disabled** | *time*] | **foreignAp** [**enabled** | **disabled** | *time*]}

Syntax Description

wlan_id	Wireless LAN identifier (1 to 512).
enabled	(Optional) Enables the exclusion list for the specified wireless LAN or foreign access point.
disabled	(Optional) Disables the exclusion list for the specified wireless LAN or a foreign access point.
time	(Optional) Exclusion list timeout in seconds. A value of zero (0) specifies infinite time.
foreignAp	Specifies a third-party access point.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

This command replaces the **config wlan blacklist** command.

The following example shows how to enable the exclusion list for WLAN ID 1:

```
(Cisco Controller) >config wlan exclusionlist 1 enabled
```

config wlan fabric

To enable or disable fabric on a WLAN, use the **config wlan fabric** command.

config wlan fabric {**enable** | **disable**} *wlan-id*

Syntax Description

enable	Enables fabric on a WLAN.
disable	Disables fabric on a WLAN.
wlan-id	WLAN identifier.

Command Default

Command Modes

Command History

Release	Modification
8.5	This command was introduced.

Usage Guidelines

Non-fabric APs are not configured with fabric WLAN.

Example

The following example shows how to enable fabric on a WLAN:

```
config wlan fabric enable wlan1
```

config wlan fabric acl

To configure access control list (ACL) name for the fabric WLAN, use the **config wlan fabric acl** command.

config wlan fabric acl *flex-acl-name* *wlan-id*

Syntax Description

flex-acl-name	ACL name.
wlan-id	WLAN identifier.

Command Default

Command Modes

Command History

Release	Modification
8.5	This command was introduced.

Usage Guidelines

The ACL to be used comes from the Flex ACL table.

Examples

The following example shows how to configure an ACL name for the fabric WLAN:

```
(Cisco Controller) >config wlan fabric acl flexACL wlan1
```

config wlan fabric avc-policy

To configure an Application Visibility and Control (AVC) profile name for the fabric WLAN, use the **config wlan fabric avc-policy** command.

config wlan fabric avc-policy *flex-avc-policy-name wlan-id*

Syntax Description

flex-avc-policy-name	AVC policy name.
wlan-id	WLAN identifier.

Command Default

None

Command History

Release	Modification
8.5	This command was introduced.

Examples

The following example shows how to configure an AVC profile name for the fabric WLAN:

```
(Cisco Controller) >config wlan fabric acl AVCpolicy wlan1
```

config wlan fabric encap vxlan

To map a Virtual Extensible LAN (VXLAN) network identifier (VNID) to a WLAN, use the **config wlan fabric encap vxlan** command.

config wlan fabric encap vxlan*wlan-id*

Syntax Description

wlan-id	WLAN identifier.

Command Default

None

Command History

Release	Modification
8.5	This command was introduced.

Examples

The following example shows how to map a VNID to a WLAN:

```
(Cisco Controller) >config wlan fabric encap vxlan wlan1
```

config wlan fabric switch-ip

To configure the IP address of the Fabric Switch that is used for the AP VXLAN tunnel, use the **config wlan fabric switch-ip** command.

config wlan fabric switch-ip *ip-address wlan-id*

Syntax Description

ip-address	IP address of the switch.
wlan-id	WLAN identifier.

Command Default

Command Modes

Command History

Release	Modification
8.5	This command was introduced.

Usage Guidelines

This command is optional for the fabric configuration, and is mainly used for guest AP tunnel. If fabric is enabled, the Switch IP where AP is connected is searched by default. You can set IP as 0.0.0.0 to disable the configuration and revert to the default configuration.

Examples

The following example shows how to configure the IP address of the Fabric Switch that is used for the AP VXLAN tunnel:

```
(Cisco Controller) >config wlan fabric switch-ip 209.165.200.224 wlan1
```

config wlan fabric tag

To configure security group tag (SGT) on a WLAN, use the **config wlan fabric tag** command.

config wlan fabric tag *sgt* *wlan-id*

Syntax Description

sgt	Security group tag.
wlan-id	WLAN identifier.

Command Default

None

Command History

Release	Modification
8.5	This command was introduced.

Usage Guidelines

To disable SGT on a WLAN, use zero at the *sgt* variable.

Ideally SGT should be acquired during authentication from the RADIUS server. For guests, this value can be configured. The default value is 0.

Examples

The following example shows how to configure SGT on a WLAN:

```
(Cisco Controller) >config wlan fabric tag sgt1 wlan1
```

The following example shows how to disable SGT from a WLAN:

```
(Cisco Controller) >config wlan fabric tag 0 wlan1
```

config wlan fabric vnid

To configure Virtual Extensible LAN (VXLAN) network identifier (VNID) on a fabric WLAN, use the **config wlan fabric vnid** command.

config wlan fabric vnid *vnid* *wlan-id*

Syntax Description

vnid	VXLAN network identifier.
wlan-id	WLAN identifier.

Command Default

None

Command History

Release	Modification
8.5	This command was introduced.

Usage Guidelines

To remove VXLAN mapping from a WLAN, use zero at the *vnid* variable.

The interface or VLAN mapping on the WLAN will be done on the switch.

Examples

The following example shows how to config VNID on a fabric WLAN:

```
(Cisco Controller) >config wlan fabric vnid1 wlan1
```

The following example shows how to remove VNID mapping from a fabric WLAN:

```
(Cisco Controller) >config wlan fabric 0 wlan1
```

config wlan flexconnect ap-auth

To configure local authentication of clients associated with FlexConnect on a locally switched WLAN, use the **config wlan flexconnect ap-auth** command.

config wlan flexconnect ap-auth *wlan_id* {**enable** | **disable**}

Syntax Description

ap-auth	Configures local authentication of clients associated with an FlexConnect on a locally switched WLAN.
wlan_id	Wireless LAN identifier between 1 and 512.
enable	Enables AP authentication on a WLAN.
disable	Disables AP authentication on a WLAN.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Local switching must be enabled on the WLAN where you want to configure local authentication of clients associated with FlexConnect.

The following example shows how to enable authentication of clients associated with FlexConnect on a specified WLAN:

```
(Cisco Controller) >config wlan flexconnect ap-auth 6 enable
```

config wlan flexconnect central-assoc

To configure client reassociation and security key caching on the controller, use the **config wlan flexconnect central-assoc** command.

config wlan flexconnect central-assoc *wlan-id* {**enable** | **disable**}

Syntax Description

wlan-id	ID of the WLAN
enable	Enables client reassociation and security key caching on the Cisco WLC
disable	Disables client reassociation and security key caching on the Cisco WLC

Command Default

Client reassociation and security key caching on the Cisco WLC is in disabled state.

Command History

Release	Modification
8.0	This command was introduced.

Usage Guidelines

A use case for this configuration is a large-scale deployment with fast roaming.

Configuration of central association with local authentication is not supported for the WLAN. After the PMIPv6 tunnel is set up, all data traffic from the PMIPv6 clients are forwarded from the Cisco AP to the local mobility anchor (LMA) in the Generic Routing Encapsulation (GRE) tunnel. If the connectivity between the Cisco AP and the Cisco WLC is lost, the data traffic for the existing PMIPv6 clients continue to flow until the connectivity between the Cisco AP and the client is lost. When the AP is in stand-alone mode, no new client associations are accepted on the PMIPv6 enabled WLAN.

The following example shows how to enable client reassociation and security key caching on the controller for a WLAN whose ID is 2:

```
(Cisco Controller) >config wlan flexconnect central-assoc 2 enable
```

config wlan flexconnect learn-ipaddr

To enable or disable client IP address learning for the Cisco WLAN controller, use the **config wlan flexconnect learn-ipaddr** command.

config wlan flexconnect learn-ipaddr *wlan_id* {**enable** | **disable**}

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.
enable	Enables client IPv4 address learning on a wireless LAN.
disable	Disables client IPv4 address learning on a wireless LAN.

Command Default

Disabled when the **config wlan flexconnect local-switching** command is disabled. Enabled when the **config wlan flexconnect local-switching** command is enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports only IPv4 address format.

Usage Guidelines

If the client is configured with Layer 2 encryption, the controller cannot learn the client IP address, and the controller will periodically drop the client. Disable this option to keep the client connection without waiting to learn the client IP address.

Note This command is valid only for IPv4.

Note The ability to disable IP address learning is not supported with FlexConnect central switching.

The following example shows how to disable client IP address learning for WLAN 6:

```
(Cisco Controller) >config wlan flexconnect learn-ipaddr disable 6
```

Related Commands

show wlan

config wlan flexconnect local-switching

To configure local switching, central DHCP, NAT-PAT, or the override DNS option on a FlexConnect WLAN, use the **config wlan flexconnect local switching** command.

config wlan flexconnect local-switching *wlan_id* {**enable** | **disable**} { {**central-dhcp** {**enable** | **disable**} **nat-pat** {**enable** | **disable**} } | {**override option dns** { **enable** | **disable**} } }

Syntax Description

wlan_id	Wireless LAN identifier from 1 to 512.
enable	Enables local switching on a FlexConnect WLAN.
disable	Disables local switching on a FlexConnect WLAN.
central-dhcp	Configures central switching of DHCP packets on the local swit When you enable this feature, the DHCP packets received from to the controller and forwarded to the corresponding VLAN base
enable	Enables central DHCP on a FlexConnect WLAN.
disable	Disables central DHCP on a FlexConnect WLAN.
nat-pat	Configures Network Address Translation (NAT) and Port Addre local switching FlexConnect WLAN.
enable	Enables NAT-PAT on the FlexConnect WLAN.
disable	Disables NAT-PAT on the FlexConnect WLAN.
override	Specifies the DHCP override options on the FlexConnect WLAN
option dns	Specifies the override DNS option on the FlexConnect WLAN. the clients get their DNS server IP address from the AP, not from
enable	Enables the override DNS option on the FlexConnect WLAN.
disable	Disables the override DNS option on the FlexConnect WLAN.

Command Default

This feature is disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports only IPv4 address format.

Usage Guidelines

When you enable the **config wlan flexconnect local-switching** command, the **config wlan flexconnect learn-ipaddr** command is enabled by default.

Note This command is valid only for IPv4.

Note The ability to disable IP address learning is not supported with FlexConnect central switching.

The following example shows how to enable WLAN 6 for local switching and enable central DHCP and NAT-PAT:

```
(Cisco Controller) >config wlan flexconnect local-switching 6 enable central-dhcp enable
nat-pat enable
```

The following example shows how to enable the override DNS option on WLAN 6:

```
(Cisco Controller) >config wlan flexconnect local-switching 6 override option dns enable
```

config wlan flexconnect vlan-central-switching

To configure central switching on a locally switched WLAN, use the **config wlan flexconnect vlan-central-switching** command.

config wlan flexconnect vlan-central-switching *wlan_id* { **enable** | **disable** }

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.
enable	Enables central switching on a locally switched wireless LAN.
disable	Disables central switching on a locally switched wireless LAN.

Command Default

Central switching is disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

You must enable Flexconnect local switching to enable VLAN central switching. When you enable WLAN central switching, the access point bridges the traffic locally if the WLAN is configured on the local IEEE 802.1Q link. If the VLAN is not configured on the access point, the AP tunnels the traffic back to the controller and the controller bridges the traffic to the corresponding VLAN.

WLAN central switching does not support:

- FlexConnect local authentication.
- Layer 3 roaming of local switching client.

The following example shows how to enable WLAN 6 for central switching:

```
(Cisco Controller) >config wlan flexconnect vlan-central-switching 6 enable
```

config wlan flow

To associate a NetFlow monitor with a WLAN, use the **config wlan flow** command.

config wlan flow *wlan_id* **monitor** *monitor_name* {**enable** | **disable**}

Syntax Description

wlan_id	Wireless LAN identifier from 1 to 512 (inclusive).
monitor	Configures a NetFlow monitor.
monitor_name	Name of the NetFlow monitor. The monitor name can be up to 32 case-sensitive, alphanumeric characters. You cannot include spaces for a monitor name.
enable	Associates a NetFlow monitor with a WLAN.
disable	Dissociates a NetFlow monitor from a WLAN.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

You can use the **config flow** command to create a new NetFlow monitor.

The following example shows how to associate a NetFlow monitor with a WLAN:

```
(Cisco Controller) >config wlan flow 5 monitor monitor1 enable
```

config wlan hotspot

To configure a HotSpot on a WLAN, use the **config wlan hotspot** command.

config wlan hotspot {**clear-all** *wlan_id* | **dot11u** | **hs2** | **msap**}

Syntax Description

clear-all	Clears the HotSpot configurations on a WLAN.
wlan_id	Wireless LAN identifier from 1 to 512.
dot11u	Configures an 802.11u HotSpot on a WLAN.
hs2	Configures HotSpot2 on a WLAN.
msap	Configures the Mobility Services Advertisement Protocol (MSAP) on a WLAN.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

You can configure up to 32 HotSpot WLANs.

The following example shows how to configure HotSpot2 for a WLAN:

```
(Cisco Controller) >config wlan hotspot hs2 enable 2
```

config wlan hotspot dot11u

To configure an 802.11u HotSpot on a WLAN, use the **config wlan hotspot dot11u** command.

config wlan hotspot dot11u {**3gpp-info** | **auth-type** | **enable** | **disable** | **domain** | **hessid** | **ipaddr-type** | **nai-realm** | **network-type** | **roam-oi**}

Syntax Description

3gpp-info	Configures 3GPP cellular network information.
auth-type	Configures the network authentication type.
disable	Disables 802.11u on the HotSpot profile.
domain	Configures a domain.
enable	Enables 802.11u on the HotSpot profile. IEEE 802.11u enables automatic WLAN offload for 802.1X devices at the HotSpot of mobile or roaming partners.
hessid	Configures the Homogenous Extended Service Set Identifier (HESSID). The HESSID is a 6-octet MAC address that uniquely identifies the network.
ipaddr-type	Configures the IPv4 address availability type.
nai-realm	Configures a realm for 802.11u enabled WLANs.
network-type	Configures the 802.11u network type and Internet access.
roam-oi	Configures the roaming consortium Organizational Identifier (OI) list.

Command Default

None.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports only IPv4 address format.

The following example shows how to enable 802.11u on a HotSpot profile:

```
(Cisco Controller) >config wlan hotspot dot11u enable 6
```

config wlan hotspot dot11u 3gpp-info

To configure 3GPP cellular network information on an 802.11u HotSpot WLAN, use the **config wlan hotspot dot11u 3gpp-info** command.

config wlan hotspot dot11u 3gpp-info {**add** | **delete**} *index country_code network_code wlan_id*

Syntax Description

add	Adds mobile cellular network information.
delete	Deletes mobile cellular network information.
index	Cellular index. The range is from 1 to 32.
country_code	Mobile Country Code (MCC) in Binary Coded Decimal (BCD) format. The country code can be up to 3 characters. For example, the MCC for USA is 310.
network_code	Mobile Network Code (MNC) in BCD format. An MNC is used in combination with a Mobile Country Code (MCC) to uniquely identify a mobile phone operator or carrier. The network code can be up to 3 characters. For example, the MNC for T- Mobile is 026.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Number of mobile network codes supported is 32 per WLAN.

The following example shows how to configure 3GPP cellular network information on a WLAN:

```
(Cisco Controller) >config wlan hotspot dot11u 3gpp-info add
```

config wlan hotspot dot11u auth-type

To configure the network authentication type on an 802.11u HotSpot WLAN, use the **config wlan hotspot dot11u auth-type** command.

config wlan hotspot dot11u auth-type *network-auth wlan_id*

Syntax Description

network-auth	Network authentication that you would like to configure on the WLAN. The available values are as follows: • 0—Acceptance of terms and conditions • 1—On-line enrollment • 2—HTTP/HTTPS redirection • 3—DNS Redirection • 4—Not Applicable
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

The DNS redirection option is not supported in Release 7.3.

The following example shows how to configure HTTP/HTTPS redirection as the network authentication type on an 802.11u HotSpot WLAN:

```
(Cisco Controller) >config wlan hotspot dot11u auth-type 2 1
```

config wlan hotspot dot11u disable

To disable an 802.11u HotSpot on a WLAN, use the **config wlan hotspot dot11u disable** command.

config wlan hotspot dot11u disable *wlan_id*

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to disable an 802.11u HotSpot on a WLAN:

```
(Cisco Controller) >config wlan hotspot dot11u disable 6
```

config wlan hotspot dot11u domain

To configure a domain operating in the 802.11 access network, use the **config wlan hotspot dot11u domain** command.

config wlan hotspot dot11u domain {**add** *wlan_id domain-index domain_name* | **delete** *wlan_id domain-index* | **modify** *wlan_id domain-index domain_name*}

Syntax Description

add	Adds a domain.
wlan_id	Wireless LAN identifier between 1 and 512.
domain-index	Domain index in the range 1 to 32.
domain_name	Domain name. The domain name is case sensitive and can be up to 255 alphanumeric characters.
delete	Deletes a domain.
modify	Modifies a domain.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to add a domain in the 802.11 access network:

```
(Cisco Controller) >config wlan hotspot dot11u domain add 6 30 domain1
```

config wlan hotspot dot11u enable

To enable an 802.11u HotSpot on a WLAN, use the **config wlan hotspot dot11u enable** command.

config wlan hotspot dot11u enable *wlan_id*

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable an 802.11u HotSpot on a WLAN:

```
(Cisco Controller) >config wlan hotspot dot11u enable 6
```

config wlan hotspot dot11u hessid

To configure a Homogenous Extended Service Set Identifier (HESSID) on an 802.11u HotSpot WLAN, use the **config wlan hotspot dot11u hessid** command.

config wlan hotspot dot11u hessid *hessid wlan_id*

Syntax Description

hessid	MAC address that can be configured as an HESSID. The HESSID is a 6-octet MAC address that uniquely identifies the network. For example, Basic Service Set Identification (BSSID) of the WLAN can be used as the HESSID.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure an HESSID on an 802.11u HotSpot WLAN:

```
(Cisco Controller) >config wlan hotspot dot11u hessid 00:21:1b:ea:36:60 6
```

config wlan hotspot dot11u ipaddr-type

To configure the type of IP address available on an 802.11u HotSpot WLAN, use the **config wlan hotspot dot11u ipaddr-type** command.

config wlan hotspot dot11u ipaddr-type *IPv4Type* {*0 - 7*} *IPv6Type* {*0 - 2*}*wlan_id*

Syntax Description

IPv4Type	IPv4 type address. Enter one of the following values: 0—IPv4 address not available. 1—Public IPv4 address available. 2—Port restricted IPv4 address available. 3—Single NAT enabled private IPv4 address available. 4—Double NAT enabled private IPv4 address available. 5—Port restricted IPv4 address and single NAT enabled IPv4 address available. 6—Port restricted IPv4 address and double NAT enabled IPv4 address available. 7— Availability of the IPv4 address is not known.
IPv6Type	IPv6 type address. Enter one of the following values: 0—IPv6 address not available. 1—IPv6 address available. 2—Availability of the IPv6 address is not known.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

The default values for IPv4 type address is 1.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports only IPv4 address format.

The following example shows how to configure the IP address availability type on an 802.11u HotSpot WLAN:

```
(Cisco Controller) >config wlan hotspot dot11u ipaddr-type 6 2 6
```

Related Commands

show wlan

config wlan hotspot dot11u nai-realm

To configure realms for an 802.11u HotSpot WLANs, use the **config wlan hotspot dot11u nai-realm** command.

config wlan hotspot dot11u nai-realm {**add** | **delete** | **modify**} {**auth-method** *wlan_id realm-index eap-index auth-index auth-method auth-parameter* | **eap-method** *wlan_id realm-index eap-index eap-method* | **realm-name** *wlan_id realm-index realm*}

Syntax Description

add	Adds a realm.
delete	Deletes a realm.
modify	Modifies a realm.
auth-method	Specifies the authentication method used.
wlan_id	Wireless LAN identifier from 1 to 512.
realm-index	Realm index. The range is from 1 to 32.
eap-index	EAP index. The range is from 1 to 4.
auth-index	Authentication index value. The range is from 1 to 10.
auth-method	Authentication method to be used. The range is from 1 to 4. The following options are available: • 1—Non-EAP Inner Auth Method • 2—Inner Auth Type • 3—Credential Type • 4—Tunneled EAP Method Credential Type
auth-parameter	Authentication parameter to use. This value depends on the authentication method used. See the following table for more details.
eap-method	Specifies the Extensible Authentication Protocol (EAP) method used.

eap-method	EAP Method. The range is from 0 to 7. The following options are available: • 0—Not Applicable • 1—Lightweight Extensible Authentication Protocol (LEAP) • 2—Protected EAP (PEAP) • 3—EAP-Transport Layer Security (EAP-TLS) • 4—EAP-FAST (Flexible Authentication via Secure Tunneling) • 5—EAP for GSM Subscriber Identity Module (EAP-SIM) • 6—EAP-Tunneled Transport Layer Security (EAP-TTLS) • 7—EAP for UMTS Authentication and Key Agreement (EAP-AKA)
realm-name	Specifies the name of the realm.
realm	Name of the realm. The realm name should be RFC 4282 compliant. For example, Cisco. The realm name is case-sensitive and can be up to 255 alphanumeric characters.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

This table lists the authentication parameters.

Table 5: Authentication Parameters

Non-EAP Inner Method(1)	Inner Authentication EAP Method Type(2)	Credential Type(3)/Tunneled EAP Credential Type(4)
0—Reserved 1—Password authentication protocol (PAP) 2—Challenge-Handshake Authentication Protocol (CHAP) 3—Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) 4—MSCHAPV2	1—LEAP 2—PEAP 3—EAP-TLS 4—EAP-FAST 5—EAP-SIM 6—EAP-TTLS 7—EAP-AKA	1—SIM 2—USIM 3—NFC Secure Element 4—Hardware Token 5—Soft Token 6—Certificate 7—Username/Password 8—Reserver 9—Anonymous 10—Vendor Specific

The following example shows how to add the Tunneled EAP Method Credential authentication method on WLAN 4:

```
(Cisco Controller) >config wlan hotspot dot11u nai-realm add auth-method 4 10 3 5 4 6
```

config wlan hotspot dot11u network-type

To configure the network type and internet availability on an 802.11u HotSpot WLAN, use the **config wlan hotspot dot11u network-type** command.

config wlan hotspot dot11u network-type *wlan_id network-type internet-access*

Syntax Description

wlan_id	Wireless LAN identifier from 1 to 512.
network-type	Network type. The available options are as follows: • 0—Private Network • 1—Private Network with Guest Access • 2—Chargeable Public Network • 3—Free Public Network • 4—Personal Device Network • 5—Emergency Services Only Network • 14—Test or Experimental • 15—Wildcard
internet-access	Internet availability status. A value of zero indicates no Internet availability and 1 indicates Internet availability.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the network type and Internet availability on an 802.11u HotSpot WLAN:

```
(Cisco Controller) >config wlan hotspot dot11u network-type 2 1
```

config wlan hotspot dot11u roam-oi

To configure a roaming consortium Organizational Identifier (OI) list on a 802.11u HotSpot WLAN, use the **config wlan hotspot dot11u roam-oi** command.

config wlan hotspot dot11u roam-oi {**add** *wlan_id oi-index oi is-beacon* | **modify** *wlan_id oi-index oi is-beacon* | **delete** *wlan_id oi-index*}

Syntax Description

add	Adds an OI.
wlan-id	Wireless LAN identifier from 1 to 512.
oi-index	Index in the range 1 to 32.
oi	Number that must be a valid 6 digit hexadecimal number and 6 bytes in length. For example, 004096 or AABBDF.
is-beacon	Beacon flag used to add an OI to the beacon. 0 indicates disable and 1 indicates enable. You can add a maximum of 3 OIs for a WLAN with this flag set.
modify	Modifies an OI.
delete	Deletes an OI.

Command Default

None.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the roaming consortium OI list:

```
(Cisco Controller) >config wlan hotspot dot11u roam-oi add 4 10 004096 1
```

config wlan hotspot hs2

To configure the HotSpot2 parameters, use the **config wlan hotspot hs2** command.

config wlan hotspot hs2 {**disable** *wlan_id* | **enable** *wlan_id* | **operator-name** {**add** *wlan_id index operator_name language-code* | **delete** *wlan_id index* | **modify** *wlan_id index operator-name language-code*} | **port-config** {**add** *wlan_id port_config_index ip-protocol port-number status* | **delete** *wlan_id port-config-index* | **modify** *wlan_id port-config-index ip-protocol port-number status*} | **wan-metrics** *wlan_id link-status symet-link downlink-speed uplink-speed* }

Syntax Description

disable	Disables HotSpot2.
wlan-id	Wireless LAN identifier from 1 to 512.
enable	Enables HotSpot2.
operator-name	Specifies the name of the 802.11 operator.
add	Adds the operator name, port configuration, or WAN metrics parameters to the WLAN configuration.
index	Index of the operator. The range is from 1 to 32.
operator-name	Name of the operator.
language-code	Language used. An ISO-14962-1997 encoded string that defines tl language. This string is a three character language code. Enter the first three letters of the language in English. For example, eng for English.
delete	Deletes the operator name, port configuration, or WAN metrics parameters from the WLAN.
modify	Modifies the operator name, port configuration, or WAN metrics parameters of the WLAN.
port-config	Configures the port configuration values.
port_config_index	Port configuration index. The range is from 1 to 32. The default value is 1.
ip-protocol	Protocol to use. This parameter provides information on the connection status of the most commonly used communication protocols and ports. The following options are available: 1—ICMP 6—FTP/SSH/TLS/PPTP-VPN/VoIP 17—IKEv2 (IPSec-VPN/VoIP/ESP) 50—ESP (IPSec-VPN)

port-number	Port number. The following options are available: 0—ICMP/ESP (IPSec-VPN) 20—FTP 22—SSH 443—TLS-VPN 500—IKEv2 1723—PPTP-VPN 4500—IKEv2 5060—VoIP
status	Status of the IP port. The following options are available: 0—Closed 1—Open 2—Unknown
wan-metrics	Configures the WAN metrics.
link-status	Link status. The following options are available: • 0—Unknown • 1—Link up • 2—Link down • 3—Link in test state
symet-link	Symmetric link status. The following options are available: • 0—Link speed is different for uplink and downlink. For example: ADSL • 1—Link speed is the same for uplink and downlink. For example: DS1
downlink-speed	Downlink speed of the WAN backhaul link in kbps. Maximum is 4,194,304 kbps.
uplink-speed	Uplink speed of the WAN backhaul link in kbps. The maximu value is 4,194,304 kbps.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the WAN metrics parameters:

```
(Cisco Controller) >config wlan hotspot hs2 wan-metrics add 345 1 0 3333
```

config wlan hotspot hs2 domain-id

To configure a domain ID, use the **config wlan hotspot hs2 domain-id** command in WLAN configuration mode.

config wlan hotspot hs2 domain-id *wlan-id domain-id*

Syntax Description

wlan-id	WLAN identification number. Enter a value between 1 and 512.
domain-id	Domain ID. Enter a value between 0 to 65535.

Command Default

The domain ID is not configured.

Command Modes

WLAN configuration

Command History

Release	Modification
Release 8.2	This command was introduced.

This example shows how to configure a domain ID:

```
Cisco Controller > config wlan hotspot hs2 domain-id 12 2
```

config wlan hotspot hs2 osu legacy-ssid

To configure Online Sign Up (OSU) Service Set Identifier (SSID) name, use the **config wlan hotspot hs2 osu legacy-ssid** command in WLAN configuration mode.

config wlan hotspot hs2 osu legacy-ssid *wlan-id ssid-name*

Syntax Description

wlan-id	WLAN identification number. Enter a value between 1 and 512.
ssid-name	SSID name.

Command Default

OSU SSID name is not configured.

Command Modes

WLAN configuration

Command History

Release	Modification
Release 8.2	This command was introduced.

This example shows how to configure an OSU SSID name:

```
Cisco Controller > config wlan hotspot hs2 osu legacy-ssid 12 cisco
```

config wlan hotspot hs2 osu sp create

To create the Online Sign Up (OSU) service provider name, use the **config wlan hotspot hs2 osu sp create** command in WLAN configuration node.

config wlan hotspot hs2 osu sp create *wlan-id osu-index lang-code* **ascii/hex** *friendly-name* [*description*]

Syntax Description

wlan-id	WLAN identification number. Enter a value between 1 and 512.
osu-index	OSU index. Enter a value between 1 and 16.
lang-code	Language code. Enter 2 or 3 letters from ISO-639, for example,*eng* for English.
ascii/hex	Specifies the text format, whether ASCII or Hex.
friendly-name	Service provider name. The maximum limit is 252 characters.
description	(Optional) Server description. The maximum limit is 252 characters.

Command Default

The OSU service provider name is not configured.

Command Modes

WLAN configuration

Command History

Release	Modification
Release 8.2	This command was introduced.

This example shows how to configure an OSU service provider name:

```
Cisco Controller > config wlan hotspot hs2 osu sp create 12 2 eng ascii cisco server-1
```

config wlan hotspot hs2 osu sp delete

To delete the Online Sign Up (OSU) service provider, use the **config wlan hotspot hs2 osu sp delete** command.

config wlan hotspot hs2 osu sp delete *wlan-idosu-index lang-code*

Syntax Description

wlan-id	WLAN identification number. Enter a value between 1 and 512.
osu-index	OSU index. Enter a value between 1 and 16.
lang-code	Language code. Enter 2 or 3 letters from ISO-639, for example, *eng* for English.

Command Default

The OSU service provider is configured.

Command Modes

WLAN configuration

Command History

Release	Modification
Release 8.2	This command was introduced.

This example shows how to delete an OSU service provider:

```
Cisco Controller > config wlan hotspot hs2 osu sp delete 12 2 eng
```

config wlan hotspot hs2 osu sp icon-file add

To configure an Online Sign Up (OSU) icon file on a particular WLAN, use the **config wlan hotspot hs2 osu sp icon-file add** command in WLAN configuration mode.

config wlan hotspot hs2 osu sp icon-file add *wlan-idosu-index icon-filename*

Syntax Description

wlan-id	WLAN identification number. Enter a value between 1 and 512.
osu-index	OSU index. Enter a value between 1 and 16.
icon-filename	Filename of the icon.

Command Default

The OSU icon file is not configured.

Command Modes

WLAN configuration

Command History

Release	Modification
Release 8.2	This command was introduced.

Usage Guidelines

Before using this command, configure icon parameters using the **config icon** *file-info* command.

This example shows how to configure an OSU icon file on a WLAN:

```
Cisco Controller > config wlan hotspot hs2 osu sp icon-file add 12 2 test-icon
```

config wlan hotspot hs2 osu sp icon-file delete

To delete an Online Sign Up (OSU) icon file from a WLAN, use the **config wlan hotspot hs2 osu sp icon-file delete** command in WLAN configuration mode.

config wlan hotspot hs2 osu sp icon-file delete *wlan-idosu-index icon-filename*

Syntax Description

wlan-id	WLAN identification number. Enter a value between 1 and 512.
osu-index	OSU index. Enter a value between 1 and 16.
icon-filename	Filename of the icon.

Command Default

The OSU icon file is configured.

Command Modes

WLAN configuration

Command History

Release	Modification
Release 8.2	This command was introduced.

This example shows how to delete an OSU icon file from a WLAN:

```
Cisco Controller > config wlan hotspot hs2 osu sp icon-file delete 12 2 test-icon
```

config wlan hotspot hs2 osu sp method add

To configure an Online Sign Up (OSU) method list, use the **config wlan hotspot hs2 osu sp method add** command in WLAN configuration mode.

config wlan hotspot hs2 osu sp method add *wlan-id osu-index method-primary method-secondary*

Syntax Description

wlan-id	WLAN identification number. Enter a value between 1 and 512.
osu-index	OSU index. Enter a value between 1 and 16.
method-primary	Primary OSU encoding method. Valid values are: **oma-dm** or **soap-xml**.
method-secondary	(Optional) Secondary OSU encoding method. Valid values are: **oma-dm** or **soap-xml**.

Command Default

The OSU method list is not configured.

Command Modes

WLAN configuration

Command History

Release	Modification
Release 8.2	This command was introduced.

This example shows how to configure an OSU method list:

```
Cisco Controller > config wlan hotspot hs2 osu sp method add 12 2 oma-dm oma-dm
```

config wlan hotspot hs2 osu sp method delete

To delete an Online Sign Up (OSU) method list, use the **config wlan hotspot hs2 osu sp method delete** command in WLAN configuration mode.

config wlan hotspot hs2 osu sp method delete *wlan-id osu-index method*

Syntax Description

wlan-id	WLAN identification number. Enter a value between 1 and 512.
osu-index	OSU index. Enter a value between 1 and 16.
method	The OSU encoding method. Valid values are **oma-dm** or **soap-xml**.

Command Default

The OSU method list is configured.

Command Modes

WLAN configuration

Command History

Release	Modification
Release 8.2	This command was introduced.

This example shows how to delete an OSU method list:

```
Cisco Controller > config wlan hotspot hs2 osu sp method delete 12 2 oma-dm
```

config wlan hotspot hs2 osu sp nai add

To create an Online Sign Up (OSU) Network Access Identifier (NAI), use the **config wlan hotspot hs2 osu sp nai add** command in WLAN configuration mode.

config wlan hotspot hs2 osu sp nai add *wlan-id osu-index nai*

Syntax Description

wlan-id	WLAN identification number. Enter a value between 1 and 512.
osu-index	OSU index. Enter a value between 1 and 16.
nai	OSU Server NAI. Enter a name within a maximum limit of 255 characters.

Command Default

The OSU NAI is not configured.

Command Modes

WLAN configuration

Command History

Release	Modification
Release 8.2	This command was introduced.

This example shows how to configure an OSU NAI:

```
Cisco Controller > config wlan hotspot hs2 osu sp nai add 12 2 nai-1
```

config wlan hotspot hs2 osu sp nai delete

To delete an Online Sign Up (OSU) Network Access Identifier (NAI), use the **config wlan hotspot hs2 osu sp nai delete** command in WLAN configuration mode.

config wlan hotspot hs2 osu sp nai delete *wlan-id osu-index*

Syntax Description

wlan-id	WLAN identification number. Enter a value between 1 and 512.
osu-index	OSU index. Enter a value between 1 and 16.

Command Default

The OSU NAI is configured.

Command Modes

WLAN configuration

Command History

Release	Modification
Release 8.2	This command was introduced.

This example shows how to delete an OSU NAI:

```
Cisco Controller > config wlan hotspot hs2 osu sp nai delete 12 2
```

config wlan hotspot hs2 osu sp uri add

To create an Online Sign Up (OSU) URI, use the **config wlan hotspot hs2 osu sp uri add** command in WLAN configuration mode.

config wlan hotspot hs2 osu sp uri add *wlan-id osu-index uri*

Syntax Description

wlan-id	WLAN identification number. Enter a value between 1 and 512.
osu-index	OSU index. Enter a value between 1 and 16.
uri	OSU server name. Enter a Uniform Resource Identifier (URI) with a maximum of 255 characters.

Command Default

The OSU URI is not configured.

Command Modes

WLAN configuration

Command History

Release	Modification
Release 8.2	This command was introduced.

This example shows how to create an OSU URI:

```
Cisco Controller > config wlan hotspot hs2 osu sp uri add 12 2 server
```

config wlan hotspot hs2 osu sp uri delete

To delete an Online Sign Up (OSU) URI, use the **config wlan hotspot hs2 osu sp uri delete** command.

config wlan hotspot hs2 osu sp uri delete *wlan-idosu-index*

Syntax Description

wlan-id	WLAN identification number. Enter a value between 1 and 512.
osu-index	OSU index. Enter a value between 1 and 16.

Command Default

The OSU URI is configured.

Command Modes

WLAN configuration

Command History

Release	Modification
Release 8.2	This command was introduced.

This example shows how to delete an OSU URI:

```
Cisco Controller > config wlan hotspot hs2 osu sp uri delete 12 2
```

config wlan hotspot hs2 wan-metrics downlink

To configure the downlink WAN metrics, use the **config wlan hotspot hs2 wan-metrics downlink** command in WLAN configuration mode.

config wlan hotspot hs2 wan-metrics downlink *wlan-id dlink-speed dlink-load*

Syntax Description

wlan-id	WLAN identification number. Enter a value between 1 and 512.
dlink-speed	WAN backhaul link speed, in Kbps. The range is from 0 to 4,294,967,295.
dlink-load	WAN backhaul link load. The range is from 0 to 100.

Command Default

The downlink WAN metrics are not configured.

Command Modes

WLAN configuration

Command History

Release	Modification
Release 8.2	This command was introduced.

This example shows how to configure downlink WAN metrics:

```
Cisco Controller > config wlan hotspot hs2 wan-metrics downlink 12 2468 10
```

config wlan hotspot hs2 wan-metrics link-status

To configure the link status of WAN metrics, use the **config wlan hotspot hs2 wan-metrics link-status** command in WLAN configuration mode.

config wlan hotspot hs2 wan-metrics link-status *wlan-id link-status*

Syntax Description

wlan-id	WLAN identification number. Enter a value between 1 and 512.
link-status	Link status. Valid values are: • **0**—Unknown • **1**—Up • **2**—Down • **3**—Test

Command Default

The link status is not configured.

Command Modes

WLAN configuration

Command History

Release	Modification
Release 8.2	This command was introduced.

This example shows how to configure the link status of WAN metrics:

```
Cisco Controller > config wlan hotspot hs2 wan-metrics link-status 12 1
```

config wlan hotspot hs2 wan-metrics lmd

To configure the load measurement duration of WAN metrics, use the **config wlan hotspot hs2 wan-metrics lmd** command in WLAN configuration mode.

config wlan hotspot hs2 wan-metrics lmd *wlan-id lmd-value*

Syntax Description

wlan-id	WLAN identification number. Enter a value between 1 and 512.
lmd-value	Load measurement duration of WAN. The range is from 0 to 65535.

Command Default

Load measurement duration of WAN is not configured.

Command Modes

WLAN configuration

Command History

Release	Modification
Release 8.2	This command was introduced.

This example shows how to configure load measurement duration of WAN metrics:

```
Cisco Controller > config wlan hotspot hs2 wan-metrics lmd 1 2456
```

config wlan hotspot hs2 wan-metrics uplink

To configure the uplink WAN metrics, use the **config wlan hotspot hs2 wan-metrics uplink** command in WLAN configuration mode.

config wlan hotspot hs2 wan-metrics uplink *wlan-id ulink-speed ulink-load*

Syntax Description

wlan-id	WLAN identification number. Enter a value between 1 and 512.
ulink-speed	WAN backhaul link speed, in Kbps. The range is from 0 to 4,294,967,295.
ulink-load	WAN backhaul link load. The range is from 0 to 100.

Command Default

The uplink WAN metrics are not configured.

Command Modes

WLAN configuration

Command History

Release	Modification
Release 8.2	This command was introduced.

This example shows how to configure the uplink WAN metrics:

```
Cisco Controller > config wlan hotspot hs2 wan-metrics uplink 12 2468 10
```

config wlan hotspot msap

To configure the Mobility Service Advertisement Protocol (MSAP) parameters on a WLAN, use the **config wlan hotspot msap** command.

config wlan hotspot msap {**enable** | **disable** | **server-id** *server_id*} *wlan_id*

Syntax Description

enable	Enables MSAP on the WLAN.
disable	Disables MSAP on the WLAN.
server-id	Specifies the MSAP server id.
server_id	MSAP server ID. The range is from 1 to 10.
wlan_id	Wireless LAN identifier from 1 to 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable MSAP on a WLAN:

```
(Cisco Controller) >config wlan hotspot msap enable 4
```

config wlan interface

To configure a wireless LAN interface or an interface group, use the **config wlan interface** command.

config wlan interface {*wlan_id* | **foreignAp**} {*interface-name* | *interface-group-name*}

Syntax Description

wlan_id	(Optional) Wireless LAN identifier (1 to 512).
foreignAp	Specifies third-party access points.
interface-name	Interface name.
interface-group-name	Interface group name.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure an interface named VLAN901:

```
(Cisco Controller) >config wlan interface 16 VLAN901
```

config wlan ipv6 acl

To configure IPv6 access control list (ACL) on a wireless LAN, use the **config wlan ipv6 acl** command.

config wlan ipv6 acl *wlan_id acl_name*

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.
acl_name	IPv6 ACL name.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure an IPv6 ACL for local switching:

```
(Cisco Controller) >config wlan ipv6 acl 22 acl_sample
```

config wlan kts-cac

To configure the Key Telephone System-based CAC policy for a WLAN, use the **config wlan kts-cac** command.

config wlan kts-cac {**enable** | **disable**} *wlan_id*

Syntax Description

enable	Enables the KTS-based CAC policy.
disable	Disables the KTS-based CAC policy.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

To enable the KTS-based CAC policy for a WLAN, ensure that you do the following:

- Configure the QoS profile for the WLAN to Platinum by entering the following command:

  config wlan qos *wlan-id* **platinum**

- Disable the WLAN by entering the following command:

  config wlan disable *wlan-id*

- Disable FlexConnect local switching for the WLAN by entering the following command:

  config wlan flexconnect local-switching *wlan-id* **disable**

The following example shows how to enable the KTS-based CAC policy for a WLAN with the ID 4:

```
(Cisco Controller) >config wlan kts-cac enable 4
```

config wlan layer2 acl

To configure a Layer 2 access control list (ACL) on a centrally switched WLAN, use the **config wlan acl layer2** command.

config wlan layer2 acl*wlan_id* {*acl_name* | **none**}

Syntax Description

wlan_id	Wireless LAN identifier. The range is from 1 to 512.
acl_name	Layer2 ACL name. The name can be up to 32 alphanumeric characters.
none	Clears any Layer2 ACL mapped to the WLAN.

Command Default

None

Command History

Release	Modification
7.5	This command was introduced.

Usage Guidelines

You can create a maximum of 16 rules for a Layer 2 ACL.

You can create a maximum of 64 Layer 2 ACLs on a Cisco WLC.

A maximum of 16 Layer 2 ACLs are supported per access point because an access point supports a maximum of 16 WLANs.

Ensure that the Layer 2 ACL names do not conflict with the FlexConnect ACL names because an access point does not support the same Layer 2 and Layer 3 ACL names.

The following example shows how to apply a Layer 2 ACL on a WLAN:

```
(Cisco Controller) >config wlan layer2 acl 1 acl_l2_1
```

config wlan ldap

To add or delete a link to a configured Lightweight Directory Access Protocol (LDAP) server, use the **config wlan ldap** command.

config wlan ldap {**add** *wlan_id server_id* | **delete** *wlan_id* {**all** | *server_id*}}

Syntax Description

add	Adds a link to a configured LDAP server.
wlan_id	Wireless LAN identifier between 1 and 512.
server_id	LDAP server index.
delete	Removes the link to a configured LDAP server.
all	Specifies all LDAP servers.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Use this command to specify the LDAP server priority for the WLAN.

To specify the LDAP server priority, one of the following must be configured and enabled:

- 802.1X authentication and Local EAP
- Web authentication and LDAP

Note Local EAP was introduced in controller software release 4.1; LDAP support on Web authentication was introduced in controller software release 4.2.

The following example shows how to add a link to a configured LDAP server with the WLAN ID 100 and server ID 4:

```
(Cisco Controller) >config wlan ldap add 100 4
```

config wlan learn-ipaddr-cswlan

To configure client IP address learning on a centrally switched WLAN, use the**config wlan learn-ipaddr-cswlan** command.

config wlan learn-ipaddr-cswlan *wlan_id* {**enable** | **disable**}

Syntax Description

wlan_id	Wireless LAN identifier from 1 to 512.
enable	Enables client IPv4 address learning on the centrally switched WLAN
disable	Disables client IPv4 address learning on the centrally switched WLAN

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports only IPv4 address format.

Usage Guidelines

If the client is configured with Layer 2 encryption, the Cisco WLC cannot learn the client IP address and will periodically drop the client. Disable this option so that the Cisco WLC maintains the client connection without waiting to learn the client IP address.

The following example shows how to enable client IP address learning on a centrally switched WLAN:

```
(Cisco Controller) >config wlan learn-ipaddr-cswlan 2 enable
```

Related Commands

show wlan

config wlan load-balance

To override the global load balance configuration and enable or disable load balancing on a particular WLAN, use the **config wlan load-balance** command.

config wlan load-balance allow {**enable** | **disable**} *wlan_id*

Syntax Description

enable	Enables band selection on a wireless LAN.
disable	Disables band selection on a wireless LAN.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

Load balancing is enabled by default.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable band selection on a wireless LAN with WLAN ID 3:

```
(Cisco Controller) >config wlan load-balance allow enable 3
```

config wlan lobby-admin-access

To provide admin access to the lobby user on a particular WLAN, use the **config wlan lobby-admin-access** command.

config wlan lobby-admin-access {**enable** | **disable**} *wlan_id*

Syntax Description

enable	Enables band selection on a wireless LAN.
disable	Disables band selection on a wireless LAN.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

Lobby admin user is disabled by default.

Command History

Release	Modification
8.4	This command was introduced.

The following example shows how to enable lobby admin on a WLAN:

```
(Cisco Controller) >config wlan lobby-admin-access enable 2
```

config wlan mac-filtering

To change the state of MAC filtering on a wireless LAN, use the **config wlan mac-filtering** command.

config wlan mac-filtering {**enable** | **disable**} {*wlan_id* | **foreignAp**}

Syntax Description

enable	Enables MAC filtering on a wireless LAN.
disable	Disables MAC filtering on a wireless LAN.
wlan_id	Wireless LAN identifier from 1 to 512.
foreignAp	Specifies third-party access points.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the MAC filtering on WLAN ID 1:

```
(Cisco Controller) >config wlan mac-filtering enable 1
```

config wlan max-associated-clients

To configure the maximum number of client connections on a wireless LAN, guest LAN, or remote LAN, use the **config wlan max-associated-clients** command.

config wlan max-associated-clients *max_clients wlan_id*

Syntax Description

max_clients	Maximum number of client connections to be accepted.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to specify the maximum number of client connections on WLAN ID 2:

```
(Cisco Controller) >config wlan max-associated-clients 25 2
```

config wlan max-radio-clients

To configure the maximum number of WLAN client per access point, use the **config wlan max-radio-clients** command.

config wlan max-radio-clients *max_radio_clients wlan_id*

Syntax Description

max_radio_clients	Maximum number of client connections to be accepted per access point radio. The valid range is from 1 to 200.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to specify the maximum number of client connections per access point radio on WLAN ID 2:

```
(Cisco Controller) >config wlan max-radio-clients 25 2
```

config wlan mdns

To configure an multicast DNS (mDNS) profile for a WLAN, use the **config wlan mdns** command.

config wlan mdns {**enable** | **disable** | **profile** {*profile-name* | **none**}} {*wlan_id* | **all**}

Syntax Description

enable	Enables mDNS snooping on a WLAN.
disable	Disables mDNS snooping on a WLAN.
profile	Configures an mDNS profile for a WLAN.
profile-name	Name of the mDNS profile to be associated with a WLAN.
none	Removes all existing mDNS profiles from the WLAN. You cannot configure mDNS profiles on the WLAN.
wlan_id	Wireless LAN identifier from 1 to 512.
all	Configures the mDNS profile for all WLANs.

Command Default

By default, mDNS snooping is enabled on WLANs.

Command History

Release	Modification
7.4	This command was introduced.

Usage Guidelines

You must disable the WLAN before you use this command. Clients receive service advertisements only for the services associated with the profile. The controller gives the highest priority to the profiles associated to interface groups, followed by the interface profiles, and then the WLAN profiles. Each client is mapped to a profile based on the order of priority.

The following example shows how to configure an mDNS profile for a WLAN.

```
(Cisco Controller) >config wlan mdns profile profile1 1
```

config wlan media-stream

To configure multicast-direct for a wireless LAN media stream, use the **config wlan media-stream** command.

config wlan media-stream multicast-direct {*wlan_id* | **all**} {**enable** | **disable**}

Syntax Description

multicast-direct	Configures multicast-direct for a wireless LAN media stream.
wlan_id	Wireless LAN identifier between 1 and 512.
all	Configures the wireless LAN on all media streams.
enable	Enables global multicast to unicast conversion.
disable	Disables global multicast to unicast conversion.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Media stream multicast-direct requires load based Call Admission Control (CAC) to run. WLAN quality of service (QoS) needs to be set to either gold or platinum.

The following example shows how to enable the global multicast-direct media stream with WLAN ID 2:

```
(Cisco Controller) >config wlan media-stream multicast-direct 2 enable
```

config wlan mfp

To configure management frame protection (MFP) options for the wireless LAN, use the **config wlan mfp** command.

config wlan mfp {**client** [**enable** | **disable**] *wlan_id* | **infrastructure protection** [**enable** | **disable**] *wlan_id*}

Syntax Description

client	Configures client MFP for the wireless LAN.
enable	(Optional) Enables the feature.
disable	(Optional) Disables the feature.
wlan_id	Wireless LAN identifier (1 to 512).
infrastructure protection	(Optional) Configures the infrastructure MFP for the wireless LAN.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure client management frame protection for WLAN ID 1:

```
(Cisco Controller) >config wlan mfp client enable 1
```

config wlan mobility anchor

To change the state of MAC filtering on a wireless LAN, use the **config wlan mobility anchor** command.

config wlan mobility anchor {**add** | **delete**} *wlan_id ip_addr* **priority** *priority-number*

Syntax Description

add	Enables MAC filtering on a wireless LAN.
delete	Disables MAC filtering on a wireless LAN.
wlan_id	Wireless LAN identifier between 1 and 512.
ip_addr	Member switch IPv4 address for anchoring the wireless LAN.
priority	Sets priority to the anchored wireless LAN IP address.
priority-number	Range between 1 to 3.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports only IPv4 address format.
8.1	**priority***priority number* parameter introduced.

The following example shows how to configure and set priority to the mobility wireless LAN anchor list with WLAN ID 4 and IPv4 address 192.168.0.14

```
(Cisco Controller) >config wlan mobility anchor add 4 192.168.0.14 priority 1
```

Related Commands

show wlan

config wlan mobility foreign-map

To configure interfaces or interface groups for foreign Cisco WLCs, use the **config wlan mobility foreign-map** command.

config wlan mobility foreign-map {**add** | **delete**} *wlan_id foreign_mac_address* {*interface_name* | *interface_group_name*}

Syntax Description

add	Adds an interface or interface group to the map of foreign controllers.
delete	Deletes an interface or interface group from the map of foreign controllers.
wlan_id	Wireless LAN identifier from 1 to 512.
foreign_mac_address	Foreign switch MAC address on a WLAN.
interface_name	Interface name up to 32 alphanumeric characters.
interface_group_name	Interface group name up to 32 alphanumeric characters.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to add an interface group for foreign Cisco WLCs with WLAN ID 4 and a foreign switch MAC address on WLAN 00:21:1b:ea:36:60:

```
(Cisco Controller) >config wlan mobility foreign-map add 4 00:21:1b:ea:36:60 mygroup1
```

config wlan multicast buffer

To configure the radio multicast packet buffer size, use the **config wlan multicast buffer** command.

config wlan multicast buffer {**enable** | **disable**} *buffer-size*

Syntax Description

enable	Enables the multicast interface feature for a wireless LAN.
disable	Disables the multicast interface feature on a wireless LAN.
buffer-size	Radio multicast packet buffer size. The range is from 30 to 60. Enter 0 to indicate APs will dynamically adjust the number of buffers allocated for multicast.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

The default buffer size is 30

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure radio multicast buffer settings:

```
(Cisco Controller) >config wlan multicast buffer enable 45 222
```

config wlan multicast interface

To configure a multicast interface for a wireless LAN, use the **config wlan multicast interface** command.

config wlan multicast interface *wlan_id* {**enable** | **disable**} *interface_name*

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.
enable	Enables multicast interface feature for a wireless LAN.
delete	Disables multicast interface feature on a wireless LAN.
interface_name	Interface name. **Note** The interface name can only be specified in lower case characters.

Command Default

Multicast is disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the multicast interface feature for a wireless LAN with WLAN ID 4 and interface name myinterface1:

```
(Cisco Controller) >config wlan multicast interface 4 enable myinterface1
```

config wlan mu-mimo

To enable Multi-User, Multiple-Input, Multiple-Output (MU-MIMO) on a WLAN, enter the **config wlan mu-mimo** command.

config wlan mu-mimo {**enable** | **disable**} *wlan-id*

Syntax Description

enable *wlan-id*	Enables MU-MIMO on the WLAN that is specified
disable *wlan-id*	Disables MU-MIMO on the WLAN that is specified

Command History

Release	Modification
8.1	This command was introduced.

config wlan nac

To enable or disable Network Admission Control (NAC) out-of-band support for a WLAN, use the **config wlan nac** command.

config wlan nac {**snmp** | **radius**} {**enable** | **disable**} *wlan_id*

Syntax Description

snmp	Configures SNMP NAC support.
radius	Configures RADIUS NAC support.
enable	Enables NAC for the WLAN.
disable	Disables NAC for the WLAN.
wlan_id	WLAN identifier from 1 to 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

You should enable AAA override before you enable the RADIUS NAC state. You also should disable FlexConnect local switching before you enable the RADIUS NAC state.

The following example shows how to configure SNMP NAC support for WLAN 13:

```
(Cisco Controller) >config wlan nac snmp enable 13
```

The following example shows how to configure RADIUS NAC support for WLAN 34:

```
(Cisco Controller) >config wlan nac radius enable 20
```

config wlan override-rate-limit

To override the bandwidth limits for upstream and downstream traffic per user and per service set identifier (SSID) defined in the QoS profile, use the **config wlan override-rate-limit** command.

config wlan override-rate-limit *wlan_id* { **average-data-rate** | **average-realtime-rate** | **burst-data-rate** | **burst-realtime-rate** } { **per-ssid** | **per-client** } { **downstream** | **upstream** } *rate*

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.
average-data-rate	Specifies the average data rate for TCP traffic per user or per SSID. The range is from 0 to 51,2000 Kbps.
average-realtime-rate	Specifies the average real-time data rate for UDP traffic per user or per SSID. The range is from 0 to 51,2000 Kbps.
burst-data-rate	Specifies the peak data rate for TCP traffic per user or per SSID. The range is from 0 to 51,2000 Kbps.
burst-realtime-rate	Specifies the peak real-time data rate for UDP traffic per user or per SSID. The range is from 0 to 51,2000 Kbps.
per-ssid	Configures the rate limit for an SSID per radio. The combined traffic of all clients will not exceed this limit.
per-client	Configures the rate limit for each client associated with the SSID.
downstream	Configures the rate limit for downstream traffic.
upstream	Configures the rate limit for upstream traffic.
rate	Data rate for TCP or UDP traffic per user or per SSID. The range is form 0 to 51,2000 Kbps. A value of 0 imposes no bandwidth restriction on the QoS profile.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

The rate limits are enforced by the controller and the AP. For central switching, the controller handles the downstream enforcement of per-client rate limit and the AP handles the enforcement of the upstream traffic and per-SSID rate limit for downstream traffic. When the AP enters standalone mode it handles the downstream enforcement of per-client rate limits too.

In FlexConnect local switching and standalone modes, per-client and per-SSID rate limiting is done by the AP for downstream and upstream traffic. However, in FlexConnect standalone mode, the configuration is not saved on the AP, so when the AP reloads, the configuration is lost and rate limiting does not happen after reboot.

For roaming clients, if the client roams between the APs on the same controller, same rate limit parameters are applied on the client. However, if the client roams from an anchor to a foreign controller, the per-client downstream rate limiting uses the parameters configured on the anchor controller while upstream rate limiting uses the parameters of the foreign controller.

The following example shows how to configure the burst real-time actual rate 2000 Kbps for the upstream traffic per SSID:

```
(Cisco Controller) >config wlan override-rate-limit 2 burst-realtime-rate per-ssid upstream
 2000
```

config wlan opendns-mode

To configure WLAN OpenDNS mode to force or copy or ignore the DNS to OpenDNS server access, use the **config wlan opendns-mode**command.

config wlan opendns-mode *wlan-id* { **ignore** | **force** | **copy** }

Syntax Description

wlan-id	Wireless LAN (WLAN) identifier.
ignore	Ignores the OpenDNS mode.
force	Forces the OpenDNS mode.
copy	Copies the OpenDNS mode.

Command Modes

(Controller Configuration) >

Command History

Release	Modification
8.4	This command was introduced.

Example

The following example shows how to configure per WLAN OpenDNS mode to copy DNS to OpenDNS server:

```
(Cisco Controller) > config wlan opendns-mode wlan1 copy
```

config wlan opendns-profile

To configure per WLAN OpenDNS profile to force or copy or ignore the Domain Name System (DNS) to OpenDNS server access, use the **config wlan opendns-profile** command.

config wlan opendns profile *wlan-id profile-name* {**enable** | **disable**}

Syntax Description

wlan-id	Wireless LAN network.
profile-name	OpenDNS profile name used for tracking this profile.
enable	Maps OpenDNS identity.
disable	Removes OpenDNS identity.

Command Modes

(Controller Configuration) >

Command History

Release	Modification
8.4	This command was introduced.

Usage Guidelines

None

Example

The following example shows how to configure a WLAN on OpenDNS profile to force the DNS to OpenDNS server:

```
(Cisco Controller) > config wlan opendns-profile wlan1 user1 enable
```

config wlan passive-client

To configure passive-client feature on a wireless LAN, use the **config wlan passive-client** command.

config wlan passive-client {**enable** | **disable**} *wlan_id*

Syntax Description

enable	Enables the passive-client feature on a WLAN.
disable	Disables the passive-client feature on a WLAN.
wlan_id	WLAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

You need to enable the global multicast mode and multicast-multicast mode by using the **config network multicast global** and **config network multicast mode** commands before entering this command.

Note You should configure the multicast in multicast-multicast mode only not in unicast mode. The passive client feature does not work with multicast-unicast mode in this release.

The following example shows how to configure the passive client on wireless LAN ID 2:

```
(Cisco Controller) >config wlan passive-client enable 2
```

config wlan peer-blocking

To configure peer-to-peer blocking on a WLAN, use the **config wlan peer-blocking** command.

config wlan peer-blocking {**disable** | **drop** | **forward-upstream**} *wlan_id*

Syntax Description

disable	Disables peer-to-peer blocking and bridge traffic locally within the controller whenever possible.
drop	Causes the controller to discard the packets.
forward-upstream	Causes the packets to be forwarded on the upstream VLAN. The device above the controller decides what action to take regarding the packets.
wlan_id	WLAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to disable the peer-to-peer blocking for WLAN ID 1:

```
(Cisco Controller) >config wlan peer-blocking disable 1
```

config wlan pmipv6 default-realm

To configure a default realm for a PMIPv6 WLAN, use the **config wlan pmipv6 default-realm** command.

config wlan pmipv6 default-realm { *default-realm-name* | **none** } *wlan_id*

Syntax Description

default-realm-name	Default realm name for the WLAN.
none	Clears the realm name for the WLAN.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure a default realm name on a PMIPv6 WLAN:

```
(Cisco Controller) >config wlan pmipv6 default-realm XYZ 6
```

config wlan pmipv6 mobility-type

To configure the mobility type on a WLAN, use the **config wlan pmipv6 mobility-type** command.

config wlan pmipv6 mobility-type { **none** | **pmipv6** } { *wlan_id* | **all** }

Syntax Description

none	Configures a WLAN with Simple IP mobility.
pmipv6	Configures a WLAN with PMIPv6 mobility.
all	Enables the specified type of mobility for all WLANs.
wlan_id	WLAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

You must disable the WLAN when you configure the mobility type.

The following example shows how to configure the mobility type as PMIPv6 on a WLAN:

```
(Cisco Controller) >config wlan pmipv6 mobility-type pmipv6 16
```

config wlan pmipv6 profile_name

To configure a profile name for the PMIPv6 WLAN, use the **config wlan pmipv6 profile_name** command.

config wlan pmipv6 profile_name *profile_name wlan_id*

Syntax Description

profile_name	Profile name for the PMIPv6 WLAN.
wlan_id	Wireless LAN identifier from 1 to 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

This command binds a profile name to the PMIPv6 WLAN or SSID. Each time that a mobile node associates with the controller, it uses the profile name and NAI in the trigger to the PMIPV6 module. The PMIPV6 module extracts all the profile specific parameters such as LMA IP, APN, and NAI and sends the PBU to the ASR5K.

The following example shows how to create a profile named ABC01 on a PMIPv6 WLAN:

```
(Cisco Controller) >config wlan pmipv6 profile_name ABC01 16
```

config wlan policy

To configure a policy on a WLAN, use the **config wlan policy** command.

config wlan policy {**add** | **delete**} *priority-index wlan-id*

Syntax Description

add	Adds a policy on a WLAN.
delete	Deletes an existing policy from a WLAN.
priority-index	Priority index of the policy to be configured on the WLAN. The policies are applied to the clients according to the priority index. The range is from 1 to 16.
policy_name	Name of the profiling policy.
wlan-id	WLAN identifier from 1 to 512.

Command Default

There is no WLAN policy.

Command History

Release	Modification
7.5	This command was introduced.

Usage Guidelines

You can apply up to 16 policies on a WLAN.

The following example shows how to configure a policy on a WLAN:

```
(Cisco Controller) >config wlan policy add 1 teacher_policy 1
```

config wlan profile

To edit a profile associated to a WLAN, use the **config wlan profile** command.

config wlan profile *wlan_id profile-name*

Syntax Description

wlan_id	WLAN identifier from 1 to 512.
profile-name	Name of the WLAN profile.

Command Default

None

Command History

Release	Modification
8.0	This command was introduced.

The following example shows how to edit a profile associated to a WLAN:

```
(Cisco Controller) > config wlan disable 1
(Cisco Controller) > config wlan profile 1 new_sample
(Cisco Controller) > show wlan summary

Number of WLANs.............................. 1

WLAN ID  WLAN Profile Name / SSID    Status    Interface Name    PMIPv6 Mobility
-------  -------------------------   --------  ---------------   ---------------
1        new_sample / new_samp       Disabled  management            none
```

config wlan profiling

To configure client profiling on a WLAN, use the **config wlan profiling** command.

config wlan profiling {**local** | **radius**} {**all** | **dhcp** | **http**} {**enable** | **disable**} *wlan_id*

Syntax Description

local	Configures client profiling in Local mode for a WLAN.
radius	Configures client profiling in RADIUS mode on a WLAN.
all	Configures DHCP and HTTP client profiling in a WLAN.
dhcp	Configures DHCP client profiling alone in a WLAN.
http	Configures HTTP client profiling in a WLAN.
enable	Enables the specific type of client profiling in a WLAN. When you enable HTTP profiling, the Cisco WLC collects the HTTP attributes of clients for profiling. When you enable DHCP profiling, the Cisco WLC collects the DHCP attributes of clients for profiling.
disable	Disables the specific type of client profiling in a WLAN.
wlan_id	Wireless LAN identifier from 1 to 512.

Usage Guidelines

Ensure that you have disabled the WLAN before configuring client profiling on the WLAN.

Command Default

Client profiling is disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Only clients connected to port 80 for HTTP can be profiled. IPv6 only clients are not profiled.

If a session timeout is configured for a WLAN, clients must send the HTTP traffic before the configured timeout to get profiled.

This feature is not supported on the following:

- FlexConnect Standalone mode
- FlexConnect Local Authentication

The following example shows how to enable both DHCP and HTTP profiling on a WLAN:

```
(Cisco Controller) >config wlan profiling radius all enable 6
          HTTP Profiling successfully enabled.
          DHCP Profiling successfully enabled.
```

config wlan qos

To change the quality of service (QoS) for a wireless LAN, use the **config wlan qos** command.

config wlan qos *wlan_id* {**bronze** | **silver** | **gold** | **platinum**}
config wlan qos foreignAp {**bronze** | **silver** | **gold** | **platinum**}

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.
bronze	Specifies the bronze QoS policy.
silver	Specifies the silver QoS policy.
gold	Specifies the gold QoS policy.
platinum	Specifies the platinum QoS policy.
foreignAp	Specifies third-party access points.

Command Default

The default QoS policy is silver.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to set the highest level of service on wireless LAN 1:

```
(Cisco Controller) >config wlan qos 1 gold
```

config wlan radio

To set the Cisco radio policy on a wireless LAN, use the **config wlan radio** command.

config wlan radio *wlan_id* {**all** | **802.11a** | **802.11bg** | **802.11g** | **802.11ag**}

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.
all	Configures the wireless LAN on all radio bands.
802.11a	Configures the wireless LAN on only 802.11a.
802.11bg	Configures the wireless LAN on only 802.11b/g (only 802.11b if 802.11g is disabled).
802.11g	Configures the wireless LAN on 802.11g only.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the wireless LAN on all radio bands:

```
(Cisco Controller) >config wlan radio 1 all
```

config wlan radius_server acct

To configure RADIUS accounting servers of a WLAN, use the **config wlan radius_server acct** command.

config wlan radius_server acct {**enable** | **disable**} *wlan_id* | **add** *wlan_id server_id* | **delete** *wlan_id* {**all** | *server_id*} | **framed-ipv6** { **address** | **both** | **prefix** } *wlan_id*}

Syntax Description

enable	Enables RADIUS accounting for the WLAN.
disable	Disables RADIUS accounting for the WLAN.
wlan_id	Wireless LAN identifier from 1 to 512.
add	Adds a link to a configured RADIUS accounting server.
server_id	RADIUS server index.
delete	Deletes a link to a configured RADIUS accounting server.
address	Configures an accounting framed IPv6 attribute to an IPv6 address.
both	Configures the accounting framed IPv6 attribute to an IPv6 address and prefix.
prefix	Configures the accounting framed IPv6 attribute to an IPv6 prefix.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable RADIUS accounting for the WLAN 2:

```
(Cisco Controller) >config wlan radius_server acct enable 2
```

The following example shows how to add a link to a configured RADIUS accounting server:

```
(Cisco Controller) > config wlan radius_server acct add 2 5
```

config wlan radius_server acct interim-update

To configure the interim update of a RADIUS accounting server of a WLAN, use the **config wlan radius_server acct interim-update** command.

config wlan radius_server acct interim-update {**enable** | **disable** | *interval* } *wlan_id*

Syntax Description

interim-update	Configures the interim update of the RADIUS accounting server.
enable	Enables interim update of the RADIUS accounting server for the WLAN.
disable	Disables interim update of the RADIUS accounting server for the WLAN.
interval	Interim update interval that you specify. The valid range is 60 to 3600 seconds.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

Interim update of a RADIUS accounting sever is set at 600 seconds.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to specify an interim update of 200 seconds to a RADIUS accounting server of WLAN 2:

```
(Cisco Controller) >config wlan radius_server acct interim-update 200 2
```

config wlan radius_server auth

To configure RADIUS authentication servers of a WLAN, use the **config wlan radius_server auth** command.

config wlan radius_server auth {**enable** *wlan_id* | **disable** *wlan_id*} {**add** *wlan_id server_id* | **delete** *wlan_id* {**all** | *server_id*}}

Syntax Description

auth	Configures a RADIUS authentication
enable	Enables RADIUS authentication for this WLAN.
wlan_id	Wireless LAN identifier from 1 to 512.
disable	Disables RADIUS authentication for this WLAN.
add	Adds a link to a configured RADIUS server.
server_id	RADIUS server index.
delete	Deletes a link to a configured RADIUS server.
all	Deletes all links to configured RADIUS servers.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to add a link to a configured RADIUS authentication server with WLAN ID 1 and Server ID 1:

```
(Cisco Controller) >config wlan radius_server auth add 1 1
```

config wlan radius_server overwrite-interface

To configure a wireless LAN's RADIUS dynamic interface, use the **config wlan radius_server overwrite-interface** command.

config wlan radius_server overwrite-interface {**enable** | **disable**} *wlan_id*

Syntax Description

enable	Enables RADIUS dynamic interface for this WLAN.
disable	Disables RADIUS dynamic interface for this WLAN.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

The controller uses the management interface as identity. If the RADIUS server is on a directly connected dynamic interface, the traffic is sourced from the dynamic interface. Otherwise, the management IP address is used.

If the feature is enabled, controller uses the interface specified on the WLAN configuration as identity and source for all RADIUS related traffic on the WLAN.

The following example shows how to enable RADIUS dynamic interface for a WLAN with an ID 1:

```
(Cisco Controller) >config wlan radius_server overwrite-interface enable 1
```

config wlan radius_server realm

To configure realm on a WLAN, use the **config wlan radius_server realm** command.

config wlan *radius_server***realm** {**enable** | **disable**} *wlan-id*

Syntax Description

radius_server	Radius server index. The range is from 1 to 17.
enable	Enable realm on a WLAN.
disable	Disable realm on a WLAN.
wlan-id	WLAN ID. The range is from 1 to 512.

Command Default

None

Command History

Release	Modification
8.0	This command was introduced.

The following example shows how to enable realm on a WLAN:

```
(Cisco Controller) > config wlan 2 realm enable 50
```

config wlan roamed-voice-client re-anchor

To configure a roamed voice client's reanchor policy, use the **config wlan roamed-voice-client re-anchor** command.

config wlan roamed-voice-client re-anchor {**enable** | **disable**} *wlan_id*

Syntax Description

enable	Enables the roamed client's reanchor policy.
disable	Disables the roamed client's reanchor policy.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

The roamed client reanchor policy is disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable a roamed voice client's reanchor policy where WLAN ID is 1:

```
(Cisco Controller) >config wlan roamed-voice-client re-anchor enable 1
```

config wlan security 802.1X

To change the state of 802.1X security on the wireless LAN Cisco radios, use the **config wlan security 802.1X** command.

config wlan security 802.1X {**enable** {*wlan_id* | **foreignAp**} | **disable** {*wlan_id* | **foreignAp**} | **encryption** {*wlan_id* | **foreignAp**} {**0** | **40** | **104**} | **on-macfilter-failure** {**enable** | **disable**}}

Syntax Description

enable	Enables the 802.1X settings.
wlan_id	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.
disable	Disables the 802.1X settings.
encryption	Specifies the static WEP keys and indexes.
0	Specifies a WEP key size of 0 (no encryption) bits. The default value is 104. **Note** All keys within a wireless LAN must be the same size.
40	Specifies a WEP key size of 40 bits. The default value is 104. **Note** All keys within a wireless LAN must be the same size.
104	Specifies a WEP key size of 104 bits. The default value is 104. **Note** All keys within a wireless LAN must be the same size.
on-macfilter-failure	Configures 802.1X on MAC filter failure.
enable	Enables 802.1X authentication on MAC filter failure.
disable	Disables 802.1X authentication on MAC filter failure.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

To change the encryption level of 802.1X security on the wireless LAN Cisco radios, use the following key sizes:

- 0—no 802.1X encryption.
- 40—40/64-bit encryption.

- 104—104/128-bit encryption. (This is the default encryption setting.)

The following example shows how to configure 802.1X security on WLAN ID 16.

```
(Cisco Controller) >config wlan security 802.1X enable 16
```

config wlan security ckip

To configure Cisco Key Integrity Protocol (CKIP) security options for the wireless LAN, use the **config wlan security ckip** command.

config wlan security ckip {**enable** | **disable**} *wlan_id* [**akm psk set-key** {**hex** | **ascii**} {**40** | **104**} **key** *key_index wlan_id* | **mmh-mic** {**enable** | **disable**} *wlan_id* | **kp** {**enable** | **disable**} *wlan_id*]

Syntax Description

enable	Enables CKIP security.
disable	Disables CKIP security.
wlan_id	Wireless LAN identifier from 1 to 512.
akm psk set-key	(Optional) Configures encryption key management for the CKIP wireless LAN.
hex	Specifies a hexadecimal encryption key.
ascii	Specifies an ASCII encryption key.
40	Sets the static encryption key length to 40 bits for the CKIP WLAN. 40-bit keys must contain 5 ASCII text characters or 10 hexadecimal characters.
104	Sets the static encryption key length to 104 bits for the CKIP WLAN. 104-bit keys must contain 13 ASCII text characters or 26 hexadecimal characters.
key	Specifies the CKIP WLAN key settings.
key_index	Configured PSK key index.
mmh-mic	(Optional) Configures multi-modular hash message integrity check (MMH MIC) validation for the CKIP wireless LAN.
kp	(Optional) Configures key-permutation for the CKIP wireless LAN.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure a CKIP WLAN encryption key of 104 bits (26 hexadecimal characters) for PSK key index 2 on WLAN 03:

```
(Cisco Controller) >config wlan security ckip akm psk set-key hex 104 key 2 03
```

config wlan security cond-web-redir

To enable or disable conditional web redirect, use the **config wlan security cond-web-redir** command.

config wlan security cond-web-redir {**enable** | **disable**} *wlan_id*

Syntax Description

enable	Enables conditional web redirect.
disable	Disables conditional web redirect.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the conditional web direct on WLAN ID 2:

```
(Cisco Controller) >config wlan security cond-web-redir enable 2
```

config wlan security eap-params

To configure local EAP timers on a WLAN, use the **config wlan security eap-params** command.

config wlan security eap-params { {**enable** | **disbale**} | **eapol-key-timeout***timeout* | **eap-key-retries** *retries* | **identity-request-timeout** *timeout* | **identity-request-retries** *retries* | **request-timeout** *timeout* | **request-retries** *retries*} *wlan_id*

Syntax Description

{**enable** | **disable** }	Specifies to enable or disable SSID specific EAP timeouts or retries. The default value is disabled.
eapol-key-timeout *timeout*	Specifies the amount of time (200 to 5000 milliseconds) that the controller attempts to send an EAP key over the WLAN to wireless clients using local EAP. The valid range is 200 to 5000 milliseconds. The default value is 1000 milliseconds.
eapol-key-retries *retries*	Specifies the maximum number of times (0 to 4 retries) that the controller attempts to send an EAP key over the WLAN to wireless clients using local EAP. The default value is 2.
identity-request- timeout *timeout*	Specifies the amount of time (1 to 120 seconds) that the controller attempts to send an EAP identity request to wireless clients within WLAN using local EAP. The default value is 30 seconds.
identity-request-retries *retries*	Specifies the maximum number of times (0 to 4 retries) that the controller attempts to retransmit the EAP identity request to wireless clients within WLAN using local EAP. The default value is 2.
request-timeout	Specifies the amount of time (1 to 120 seconds) in which the controller attempts to send an EAP parameter request to wireless clients within WLAN using local EAP. The default value is 30 seconds.
request-retries*retries*	Specifies the maximum number of times (0 to 20 retries) that the controller attempts to retransmit the EAP parameter request to wireless clients within WLAN using local EAP. The default value is 2.
wlan-id	WLAN identification number.

Command Default

The default EAPOL key timeout is 1000 milliseconds.

The default for EAPOL key retries is 2.

The default identity request timeout is 30 seconds.

The default identity request retries is 2.

The default request timeout is 30 seconds.

The default request retries is 2.

Command History

Release	Modification
7.6	This command was introduced.

The following example shows how to enable SSID specific EAP parameters on a WLAN:

```
(Cisco Controller) > config wlan security eap-params enable 4
```

The following example shows how to set EAPOL key timeout parameter on a WLAN:

```
(Cisco Controller) > config wlan security eap-params eapol-key-retries 4
```

The following example shows how to set EAPOL key retries on a WLAN:

```
(Cisco Controller) > config wlan security eap-params eapol-key-retries 4
```

config wlan security eap-passthru

To configure the 802.1X frames pass through on to the external authenticator, use the **config wlan security eap-passthru** command.

config wlan security eap-passthru {**enable** | **disable**} *wlan_id*

Syntax Description

enable	Enables 802.1X frames pass through to external authenticator.
disable	Disables 802.1X frames pass through to external authenticator.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the 802.1X frames pass through to external authenticator on WLAN ID 2:

```
(Cisco Controller) >config wlan security eap-passthru enable 2
```

config wlan security ft

To configure 802.11r Fast Transition Roaming parameters, use the **config wlan security ft** command.

config wlan security ft {**adaptive** | **enable** | **disable** | **reassociation-timeout** *timeout-in-seconds*} *wlan_id*

Syntax Description

adaptive	Configures 802.11r Fast Transition Roaming adaptive support. This is the default option.
enable	Enables 802.11r Fast Transition Roaming support.
disable	Disables 802.11r Fast Transition Roaming support.
reassociation-timeout	Configures reassociation deadline interval.
timeout-in-seconds	Reassociation timeout value, in seconds. The valid range is 1 to 100 seconds.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.3	This command was modified. The **adaptive** keyword was added.

Usage Guidelines

Ensure that you have disabled the WLAN before you proceed.

The following example shows how to enable 802.11r Fast Transition Roaming support on WLAN 2:

```
(Cisco Controller) >config wlan security ft enable 2
```

The following example shows how to set a reassociation timeout value of 20 seconds for 802.11r Fast Transition Roaming support on WLAN 2:

```
(Cisco Controller) >config wlan security ft reassociation-timeout 20 2
```

config wlan security ft over-the-ds

To configure 802.11r fast transition parameters over a distributed system, use the **config wlan security ft over-the-ds** command.

config wlan security ft over-the-ds {**enable** | **disable**} *wlan_id*

Syntax Description

enable	Enables 802.11r fast transition roaming support over a distributed system.
disable	Disables 802.11r fast transition roaming support over a distributed system.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

Enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Ensure that you have disabled the WLAN before you proceed.

Ensure that 802.11r fast transition is enabled on the WLAN.

The following example shows how to enable 802.11r fast transition roaming support over a distributed system on WLAN ID 2:

```
(Cisco Controller) >config wlan security ft over-the-ds enable 2
```

config wlan security IPsec disable

To disable IPsec security, use the **config wlan security IPsec disable** command.

config wlan security IPsec disable {*wlan_id* | **foreignAp**}

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to disable the IPsec for WLAN ID 16:

```
(Cisco Controller) >config wlan security IPsec disable 16
```

config wlan security IPsec enable

To enable IPsec security, use the **config wlan security IPsec enable** command.

config wlan security IPsec enable {*wlan_id* | **foreignAp**}

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the IPsec for WLAN ID 16:

```
(Cisco Controller) >config wlan security IPsec enable 16
```

config wlan security IPsec authentication

To modify the IPsec security authentication protocol used on the wireless LAN, use the **config wlan security IPsec authentication** command.

config wlan security IPsec authentication {**hmac-md5** | **hmac-sha-1**} {*wlan_id* | **foreignAp**}

Syntax Description

hmac-md5	Specifies the IPsec HMAC-MD5 authentication protocol.
hmac-sha-1	Specifies the IPsec HMAC-SHA-1 authentication protocol.
wlan_id	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the IPsec HMAC-SHA-1 security authentication parameter for WLAN ID 1:

```
(Cisco Controller) >config wlan security IPsec authentication hmac-sha-1 1
```

config wlan security IPsec encryption

To modify the IPsec security encryption protocol used on the wireless LAN, use the **config wlan security IPsec encryption** command.

config wlan security IPsec encryption {**3des** | **aes** | **des**} {*wlan_id* | **foreignAp**}

Syntax Description

3des	Enables IPsec 3DES encryption.
aes	Enables IPsec AES 128-bit encryption.
des	Enables IPsec DES encryption.
wlan_id	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the IPsec AES encryption:

```
(Cisco Controller) >config wlan security IPsec encryption aes 1
```

config wlan security IPsec config

To configure the proprietary Internet Key Exchange (IKE) CFG-Mode parameters used on the wireless LAN, use the **config wlan security IPsec config** command.

config wlan security IPsec config qotd *ip_address* {*wlan_id* | **foreignAp**}

Syntax Description

qotd	Configures the quote-of-the day server IP for cfg-mode.
ip_address	Quote-of-the-day server IP for cfg-mode.
wlan_id	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

IKE is used as a method of distributing the session keys (encryption and authentication), as well as providing a way for the VPN endpoints to agree on how the data should be protected. IKE keeps track of connections by assigning a bundle of Security Associations (SAs), to each connection.

The following example shows how to configure the quote-of-the-day server IP 44.55.66.77 for cfg-mode for WLAN 1:

```
(Cisco Controller) >config wlan security IPsec config qotd 44.55.66.77 1
```

config wlan security IPsec ike authentication

To modify the IPsec Internet Key Exchange (IKE) authentication protocol used on the wireless LAN, use the **config wlan security IPsec ike authentication** command.

config wlan security IPsec ike authentication {**certificates** {*wlan_id* | **foreignAp**} | **pre-share-key** {*wlan_id* | **foreignAp**} *key* | **xauth-psk** {*wlan_id* | **foreignAp**} *key*}

Syntax Description

certificates	Enables the IKE certificate mode.
wlan_id	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.
pre-share-key	Enables the IKE Xauth with preshared keys.
xauth-psk	Enables the IKE preshared key.
key	Key required for preshare and xauth-psk.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the IKE certification mode:

```
(Cisco Controller) >config wlan security IPsec ike authentication certificates 16
```

config wlan security IPsec ike dh-group

To modify the IPsec Internet Key Exchange (IKE) Diffie Hellman group used on the wireless LAN, use the **config wlan security IPsec ike dh-group** command.

config wlan security IPsec ike dh-group {*wlan_id* | **foreignAp**} {**group-1** | **group-2** | **group-5**}

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.
group-1	Specifies DH group 1 (768 bits).
group-2	Specifies DH group 2 (1024 bits).
group-5	Specifies DH group 5 (1536 bits).

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the Diffe Hellman group parameter for group-1:

```
(Cisco Controller) >config wlan security IPsec ike dh-group 1 group-1
```

config wlan security IPsec ike lifetime

To modify the IPsec Internet Key Exchange (IKE) lifetime used on the wireless LAN, use the **config wlan security IPsec ike lifetime** command.

config wlan security IPsec ike lifetime {*wlan_id* | **foreignAp**} *seconds*

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.
seconds	IKE lifetime in seconds, between 1800 and 345600.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the IPsec IKE lifetime use on the wireless LAN:

```
(Cisco Controller) >config wlan security IPsec ike lifetime 1 1900
```

config wlan security IPsec ike phase1

To modify IPsec Internet Key Exchange (IKE) Phase 1 used on the wireless LAN, use the **config wlan security IPsec ike phase1** command.

config wlan security IPsec ike phase1 {**aggressive** | **main**} {*wlan_id* | **foreignAp**}

Syntax Description

aggressive	Enables the IKE aggressive mode.
main	Enables the IKE main mode.
wlan_id	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to modify IPsec IKE Phase 1:

```
(Cisco Controller) >config wlan security IPsec ike phase1 aggressive 16
```

config wlan security IPsec ike contivity

To modify Nortel's Contivity VPN client support on the wireless LAN, use the **config wlan security IPsec ike contivity** command.

config wlan security IPsec ike contivity {**enable** | **disable**} {*wlan_id* | **foreignAp**}

Syntax Description

enable	Enables contivity support for this WLAN.
disable	Disables contivity support for this WLAN.
wlan_id	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to modify Contivity VPN client support:

```
(Cisco Controller) >config wlan security IPsec ike contivity enable 14
```

config wlan security wpa akm ft

To configure authentication key-management using 802.11r fast transition 802.1X, use the **config wlan security wpa akm ft** command.

config wlan security wpa akm ft [**over-the-air** | **over-the-ds** | **psk** | [**reassociation-timeout** *seconds*]] {**enable** | **disable**} *wlan_id*

Syntax Description

over-the-air	(Optional) Configures 802.11r fast transition roaming over-the-air support.
over-the-ds	(Optional) Configures 802.11r fast transition roaming DS support.
psk	(Optional) Configures 802.11r fast transition PSK support.
reassociation-timeout	(Optional) Configures the reassociation deadline interval. The valid range is between 1 to 100 seconds. The default value is 20 seconds.
seconds	Reassociation deadline interval in seconds.
enable	Enables 802.11r fast transition 802.1X support.
disable	Disables 802.11r fast transition 802.1X support.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure authentication key-management using 802.11r fast transition:

```
(Cisco Controller) >config wlan security wpa akm ft reassociation-timeout 25 1
```

config wlan security ft

To configure 802.11r Fast Transition Roaming parameters, use the **config wlan security ft** command.

config wlan security ft {**adaptive** | **enable** | **disable** | **reassociation-timeout** *timeout-in-seconds*} *wlan_id*

Syntax Description

adaptive	Configures 802.11r Fast Transition Roaming adaptive support. This is the default option.
enable	Enables 802.11r Fast Transition Roaming support.
disable	Disables 802.11r Fast Transition Roaming support.
reassociation-timeout	Configures reassociation deadline interval.
timeout-in-seconds	Reassociation timeout value, in seconds. The valid range is 1 to 100 seconds.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.3	This command was modified. The **adaptive** keyword was added.

Usage Guidelines

Ensure that you have disabled the WLAN before you proceed.

The following example shows how to enable 802.11r Fast Transition Roaming support on WLAN 2:

```
(Cisco Controller) >config wlan security ft enable 2
```

The following example shows how to set a reassociation timeout value of 20 seconds for 802.11r Fast Transition Roaming support on WLAN 2:

```
(Cisco Controller) >config wlan security ft reassociation-timeout 20 2
```

config wlan security passthru

To modify the IPsec pass-through used on the wireless LAN, use the **config wlan security passthru** command.

config wlan security passthru {**enable** | **disable**} {*wlan_id* | **foreignAp**} [*ip_address*]

Syntax Description

enable	Enables IPsec pass-through.
disable	Disables IPsec pass-through.
wlan_id	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.
ip_address	(Optional) IP address of the IPsec gateway (router) that is terminating the VPN tunnel.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to modify IPsec pass-through used on the wireless LAN:

```
(Cisco Controller) >config wlan security passthru enable 3 192.12.1.1
```

config wlan security pmf

To configure 802.11w Management Frame Protection (MFP) on a WLAN, use the **config wlan security pmf** command.

config wlan security pmf {**disable** | **optional** | **required** | **association-comeback** *association-comeback_timeout* | **saquery-retrytimeout** *saquery-retry_timeout*} *wlan_id*

Syntax Description

disable	Disables 802.11w MFP protection on a WLAN.
optional	Enables 802.11w MFP protection on a WLAN.
required	Requires clients to negotiate 802.11w MFP protection on a WLAN.
association-comeback	Configures the 802.11w association comeback time.
association-comeback_timeout	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 to 20 seconds.
saquery-retrytimeout	Configures the 802.11w Security Association (SA) query retry timeout.
saquery-retry_timeout	Time interval identified in the association response to an already associated client before the association can be tried again. This time interval checks if the client is a real client and not a rogue client during the association comeback time. If the client does not respond within this time, the client association is deleted from the controller. The range is from 100 to 500 ms.
wlan_id	Wireless LAN identifier from 1 to 512.

Command Default

Default SA query retry timeout is 200 milliseconds.

Default association comeback timeout is 1 second.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

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 WPA or WPA2 security at Layer 2.

The following example shows how to enable 802.11w MFP protection on a WLAN:

```
(Cisco Controller) > config wlan security pmf optional 1
```

The following example shows how to configure the SA query retry timeout on a WLAN:

```
(Cisco Controller) > config wlan security pmf saquery-retrytimeout 300 1
```

config wlan security sgt

To configures Secure Group Tag (SGT) for a WLAN, use the **config wlan security sgt** command.

config wlan security sgt {*value* | *wlan-id*} *wlan_id*

Syntax Description

value	SGT value
wlan-id	WLAN ID

Command Default

None

Command History

Release	Modification
8.4	This command was introduced

config wlan security splash-page-web-redir

To enable or disable splash page web redirect, use the **config wlan security splash-page-web-redir** command.

config wlan security splash-page-web-redir {**enable** | **disable**} *wlan_id*

Syntax Description

enable	Enables splash page web redirect.
disable	Disables splash page web redirect.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

Splash page web redirect is disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable spash page web redirect:

```
(Cisco Controller) >config wlan security splash-page-web-redir enable 2
```

config wlan security static-wep-key authentication

To configure static Wired Equivalent Privacy (WEP) key 802.11 authentication on a wireless LAN, use the **config wlan security static-wep-key authentication** command.

config wlan security static-wep-key authentication {**shared-key** | **open**} *wlan_id*

Syntax Description

shared-key	Enables shared key authentication.
open	Enables open system authentication.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the static WEP shared key authentication for WLAN ID 1:

```
(Cisco Controller) >config wlan security static-wep-key authentication shared-key 1
```

config wlan security static-wep-key disable

To disable the use of static Wired Equivalent Privacy (WEP) keys, use the **config wlan security static-wep-key disable** command.

config wlan security static-wep-key disable *wlan_id*

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to disable the static WEP keys for WLAN ID 1:

```
(Cisco Controller) >config wlan security static-wep-key disable 1
```

config wlan security static-wep-key enable

To enable the use of static Wired Equivalent Privacy (WEP) keys, use the **config wlan security static-wep-key enable** command.

config wlan security static-wep-key enable *wlan_id*

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the use of static WEK keys for WLAN ID 1:

```
(Cisco Controller) >config wlan security static-wep-key enable 1
```

config wlan security static-wep-key encryption

To configure the static Wired Equivalent Privacy (WEP) keys and indexes, use the **config wlan security static-wep-key encryption** command.

config wlan security static-wep-key encryption *wlan_id* {**40** | **104**} {**hex** | **ascii**} *key key-index*

Syntax Description

wlan_id	Wireless LAN identifier from 1 to 512.
40	Specifies the encryption level of 40.
104	Specifies the encryption level of 104.
hex	Specifies to use hexadecimal characters to enter key.
ascii	Specifies whether to use ASCII characters to enter key.
key	WEP key in ASCII.
key-index	Key index (1 to 4).

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

One unique WEP key index can be applied to each wireless LAN. Because there are only four WEP key indexes, only four wireless LANs can be configured for static WEP Layer 2 encryption.

Make sure to disable 802.1X before using this command.

The following example shows how to configure the static WEP keys for WLAN ID 1 that uses hexadecimal character 0201702001 and key index 2:

```
(Cisco Controller) >config wlan security static-wep-key encryption 1 40 hex 0201702001 2
```

config wlan security tkip

To configure the Temporal Key Integrity Protocol (TKIP) Message Integrity Check (MIC) countermeasure hold-down timer, use the **config wlan security tkip** command.

config wlan security tkip hold-down *time wlan_id*

Syntax Description

hold-down	Configures the TKIP MIC countermeasure hold-down timer.
time	TKIP MIC countermeasure hold-down time in seconds. The range is from 0 to 60 seconds.
wlan_id	Wireless LAN identifier from 1 to 512.

Command Default

The default TKIP countermeasure is set to 60 seconds.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

TKIP countermeasure mode can occur if the access point receives 2 MIC errors within a 60 second period. When this situation occurs, the access point deauthenticates all TKIP clients that are associated to that 802.11 radio and holds off any clients for the countermeasure holdoff time.

The following example shows how to configure the TKIP MIC countermeasure hold-down timer:

```
(Cisco Controller) >config wlan security tkip
```

config wlan usertimeout

To configure the timeout for idle client sessions for a WLAN, use the **config wlan usertimeout** command.

config wlan usertimeout *timeout wlan_id*

Syntax Description

timeout	Timeout for idle client sessions for a WLAN. If the client sends traffic less than the threshold, the client is removed on timeout. The range is from 15 to 100000 seconds.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

The default client session idle timeout is 300 seconds.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

The timeout value that you configure here overrides the global timeout that you define using the command **config network usertimeout**.

The following example shows how to configure the idle client sessions for a WLAN:

```
(Cisco Controller) >config wlan usertimeout 100 1
```

config wlan security web-auth

To change the status of web authentication used on a wireless LAN, use the **config wlan security web-auth** command.

config wlan security web-auth {{**acl** | **enable** | **disable**} {*wlan_id* | **foreignAp**} [*acl_name* | **none**]} | {**on-macfilter-failure** *wlan_id*} | {**server-precedence** *wlan_id* | **local** | **ldap** | **radius**} | {**flexacl** *wlan_id* [*ipv4_acl_name* | **none**]} | {**ipv6 acl** *wlan_id* [*ipv6_acl_name* | **none**]} | {**mac-auth-server** {*ip_address wlan_id* }} | {**timeout** {*value_in_seconds wlan_id* }} | {**web-portal-server** {*ip_address wlan_id* }}

Syntax Description

acl	Configures the access control list.
enable	Enables web authentication.
disable	Disables web authentication.
wlan_id	Wireless LAN identifier from 1 to 512.
foreignAp	Specifies third-party access points.
acl_name	(Optional) ACL name (up to 32 alphanumeric characters).
none	(Optional) Specifies no ACL name.
on-macfilter-failure	Enables web authentication on MAC filter failure.
server-precendence	Configures the authentication server precedence order for Web-Auth users.
local	Specifies the server type.
ldap	Specifies the server type.
radius	Specifies the server type.
flexacl	Configures Flexconnect Access Control List.
ipv4_acl_name	(Optional) IPv4 ACL name. You can enter up to 32 alphanumeric characters.
ipv6_acl_name	(Optional) IPv6 ACL name. You can enter up to 32 alphanumeric characters.
ipv6	Configures IPv6 related parameters.
mac-auth-server	Configures MAC authentication server for the WLAN.

timeout	Configures Local Web authentication Timeout. **Note** The CWA session timeout is fixed to 600 seconds.
value_in_seconds	Timeout value in seconds; valid range is between 300 and 14400 seconds.
web-portal-server	Configures CMCC web portal server for the WLAN.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the security policy for WLAN ID 1 and an ACL named ACL03:

```
(Cisco Controller) >config wlan security web-auth acl 1 ACL03
```

config wlan security web-auth captive-bypass

To configure captive-bypass on a wireless LAN, use the **config wlan security web-auth captive-bypass** command.

config wlan security web-auth captive-bypass {**enable | disable | none** }

Syntax Description

enable	Enable the captive-bypass for WLAN.
disable	Disable the captive-bypass for WLAN.
none	Clear the captive-bypass configuration for WLAN. And global captive netwrok assistant bypass setting will get applied
wlan-id	Enter WLAN identifier between 1 and 16.

Command History

Release	Modification
8.4	This command is introduced.

The following example shows how to enable Captive Network Bypass:

```
(Cisco Controller) >config wlan security web-auth captive-bypass enable 1
```

config wlan security web-auth qrscan-des-key

To configure the QR-scan DES key in a WLAN, use the **config wlan security web-auth qrscan-des-key** command.

config wlan security web-auth qrscan-des-key {*DES key stringwlan_id* }

Syntax Description

DES key string	Enter the DES key of 8 characters.
wlan-id	Enter WLAN Identifier between 1 and 16.

Command History

Release	Modification
8.4	This command was introduced.

The following example shows how to configure the QR-scan DES key:

```
(Cisco Controller) >config wlan security web-auth qrscan-des-key 1
```

config wlan security web-passthrough acl

To add an access control list (ACL) to the wireless LAN definition, use the **config wlan security web-passthrough acl** command.

config wlan security web-passthrough acl {*wlan_id* | **foreignAp**} {*acl_name* | **none**}

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.
acl_name	ACL name (up to 32 alphanumeric characters).
none	Specifies that there is no ACL.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to add an ACL to the wireless LAN definition:

```
(Cisco Controller) >config wlan security web-passthrough acl 1 ACL03
```

config wlan security web-passthrough disable

To disable a web captive portal with no authentication required on a wireless LAN, use the **config wlan security web-passthrough disable** command.

config wlan security web-passthrough disable {*wlan_id* | **foreignAp**}

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to disable a web captive portal with no authentication required on wireless LAN ID 1:

```
(Cisco Controller) >config wlan security web-passthrough disable 1
```

config wlan security web-passthrough email-input

To configure a web captive portal using an e-mail address, use the **config wlan security web-passthrough email-input** command.

config wlan security web-passthrough email-input {**enable** | **disable**} {*wlan_id* | **foreignAp**}

Syntax Description

email-input	Configures a web captive portal using an e-mail address.
enable	Enables a web captive portal using an e-mail address.
disable	Disables a web captive portal using an e-mail address.
wlan_id	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure a web captive portal using an e-mail address:

```
(Cisco Controller) >config wlan security web-passthrough email-input enable 1
```

config wlan security web-passthrough enable

To enable a web captive portal with no authentication required on the wireless LAN, use the **config wlan security web-passthrough enable** command.

config wlan security web-passthrough enable {*wlan_id* | **foreignAp**}

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable a web captive portal with no authentication required on wireless LAN ID 1:

```
(Cisco Controller) >config wlan security web-passthrough enable 1
```

config wlan security web-passthrough qr-scan

To enable or disable qr-scan on the WLAN, use the **config wlan security web-passthrough qr-scan** command.

config wlan security web-passthrough qr-scan { { **localenable | disable** } | **enable | disable** }

Syntax Description

local	Configures QR code scanning support locally on AP for clients. • **enable**–enables QR code scanning support for clients. • **disable**–disables QR code scanning support for clients.
enable	Enables QR code scanning support for clients.
disable	Disables QR code scanning support for clients.
wlan-id	Enter WLAN Identifier between 1 and 16.

Command Default

None

Command History

Release	Modification
8.4	This command was introduced.

The following example shows how to enable qr-scan on WLAN ID 1:

```
(Cisco Controller) >config wlan security web-passthrough qr-scan enable 1
```

config wlan security wpa akm 802.1x

To configure authentication key-management (AKM) using 802.1X, use the **config wlan security wpa akm 802.1x** command.

config wlan security wpa akm 802.1x {**enable** | **disable**} *wlan_id*

Syntax Description

enable	Enables the 802.1X support.
disable	Disables the 802.1X support.
wlan_id	Wireless LAN identifier from 1 to 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure authentication using 802.1X.

```
(Cisco Controller) >config wlan security wpa akm 802.1x enable 1
```

config wlan security wpa akm cckm

To configure authentication key-management using Cisco Centralized Key Management (CCKM), use the **config wlan security wpa akm cckm** command.

config wlan security wpa akm cckm { **enable** *wlan_id* | **disable** *wlan_id* | *timestamp-tolerance* }

Syntax Description

enable	Enables CCKM support.
disable	Disables CCKM support.
wlan_id	Wireless LAN identifier between 1 and 512.
timestamp-tolerance	CCKM IE time-stamp tolerance. The range is between 1000 to 5000 milliseconds; the default is 1000 milliseconds.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure authentication key-management using CCKM.

```
(Cisco Controller) >config wlan security wpa akm cckm 1500
```

config wlan security wpa akm ft

To configure authentication key-management using 802.11r fast transition 802.1X, use the **config wlan security wpa akm ft** command.

config wlan security wpa akm ft [**over-the-air** | **over-the-ds** | **psk** | [**reassociation-timeout** *seconds*]] {**enable** | **disable**} *wlan_id*

Syntax Description

over-the-air	(Optional) Configures 802.11r fast transition roaming over-the-air support.
over-the-ds	(Optional) Configures 802.11r fast transition roaming DS support.
psk	(Optional) Configures 802.11r fast transition PSK support.
reassociation-timeout	(Optional) Configures the reassociation deadline interval. The valid range is between 1 to 100 seconds. The default value is 20 seconds.
seconds	Reassociation deadline interval in seconds.
enable	Enables 802.11r fast transition 802.1X support.
disable	Disables 802.11r fast transition 802.1X support.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure authentication key-management using 802.11r fast transition:

```
(Cisco Controller) >config wlan security wpa akm ft reassociation-timeout 25 1
```

config wlan security wpa akm pmf

To configure Authenticated Key Management (AKM) of management frames, use the **config wlan security wpa akm pmf** command.

config wlan security wpa akm pmf {**802.1x** | **psk**} {**enable** | **disable**} *wlan_id*

Syntax Description

802.1x	Configures 802.1X authentication for protection of management frames (PMF).
psk	Configures preshared keys (PSK) for PMF.
enable	Enables 802.1X authentication or PSK for PMF.
disable	Disables 802.1X authentication or PSK for PMF.
wlan_id	Wireless LAN identifier from 1 to 512.

Command Default

Disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

802.11w has two new AKM suites: 00-0F-AC:5 or 00-0F-AC:6. You must enable WPA and then disable the WLAN to configure PMF on the WLAN.

The following example shows how to enable 802.1X authentication for PMF in a WLAN:

```
(Cisco Controller) >config wlan security wpa akm pmf 802.1x enable 1
```

config wlan security wpa akm psk

To configure the Wi-Fi protected access (WPA) preshared key mode, use the **config wlan security wpa akm psk** command.

config wlan security wpa akm psk { { **enable** | **disable** } | { **set-key** *key-format key* } | { **auto-key** { **enable** | **disable** } } | { **pmkid** { **enable** | **disable** } } *wlan_id* }

Syntax Description

enable	Enables WPA-PSK.
disable	Disables WPA-PSK.
set-key	Configures a preshared key.
key-format	Specifies key format. Either ASCII or hexadecimal.
key	WPA preshared key.
auto-key {**enable** | **disable**}	Configures auto PSK on the WLAN.
pmkid {**enable** | **disable**}	Configures PMK ID inclusion in M1 of 4-way handshake messages.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.10	The **pmkid** {**enable** | **disable**} was introduced.

Examples

The following example shows how to configure the WPA preshared key mode:

```
(Cisco Controller) >config wlan security wpa akm psk disable 1
```

config wlan security wpa disable

To disable WPA1, use the **config wlan security wpa disable** command.

config wlan security wpa disable *wlan_id*

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to disable WPA:

```
(Cisco Controller) >config wlan security wpa disable 1
```

config wlan security wpa enable

To enable WPA1, use the **config wlan security wpa enable** command.

config wlan security wpa enable *wlan_id*

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the WPA on WLAN ID 1:

```
(Cisco Controller) >config wlan security wpa enable 1
```

config wlan security wpa ciphers

To configure the Wi-Fi protected authentication (WPA1) or Wi-Fi protected authentication (WPA2), use the **config wlan security wpa ciphers** command.

config wlan security wpa {**wpa1** | **wpa2**} **ciphers** {**aes** | **tkip**} {**enable** | **disable**} *wlan_id*

Syntax Description

wpa1	Configures WPA1 support.
wpa2	Configures WPA2 support.
ciphers	Configures WPA ciphers.
aes	Configures AES encryption support.
tkip	Configures TKIP encryption support.
enable	Enables WPA AES/TKIP mode.
disable	Disables WPA AES/TKIP mode.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

If you are not specifying the WPA versions, it implies the following:

- If the cipher enabled is AES, you are configuring WPA2/AES.
- If the ciphers enabled is AES+TKIP, you are configuring WPA/TKIP, WPA2/AES,or WPA/TKIP.
- If the cipher enabled is TKIP, you are configuring WPA/TKIP or WPA2/TKIP.

From Release 8.0, you cannot configure TKIP as a standalone encryption method. TKIP can be used only with the AES encryption method.

The following example shows how to encrypt the WPA:

```
(Cisco Controller) >config wlan security wpa wpa1 ciphers aes enable 1
```

config wlan security wpa gtk-random

To enable the randomization of group temporal keys (GTK) between access points and clients on a WLAN, use the **config wlan security wpa gtk-random** command.

config wlan security wpa gtk-random {**enable** | **disable**} *wlan_id*

Syntax Description

enable	Enables the randomization of GTK keys between the access point and clients.
disable	Disables the randomization of GTK keys between the access point and clients.
wlan_id	WLAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

When you enable this command, the clients in the Basic Service Set (BSS) get a unique GTK key. The clients do not receive multicast or broadcast traffic.

The following example shows how to enable the GTK randomization for each client associated on a WLAN:

```
(Cisco Controller) >config wlan security wpa gtk-random enable 3
```

config wlan security wpa osen disable

To disable OSU Server-Only Authenticated L2 Encryption Network (OSEN) on a WLAN, use the **config wlan security wpa osen enable** command in WLAN configuration mode.

config wlan security wpa osen disable *wlan-id*

Syntax Description

wlan-id	WLAN identification number. Enter a value between 1 and 512.

Command Default

OSEN is enabled.

Command Modes

WLAN configuration

Command History

Release	Modification
Release 8.2	This command was introduced.

This example shows how to disable OSEN on a WLAN:

```
Cisco Controller > config wlan security wpa osen disable 12
```

config wlan security wpa osen enable

To enable OSU Server-Only Authenticated L2 Encryption Network (OSEN) on a WLAN, use the **config wlan security wpa osen enable** command in WLAN configuration mode.

config wlan security wpa osen enable *wlan-id*

Syntax Description

wlan-id	WLAN identification number. Enter a value between 1 and 512.

Command Default

OSEN is not enabled.

Command Modes

WLAN configuration

Command History

Release	Modification
Release 8.2	This command was introduced.

This example shows how to enable an OSEN on a WLAN:

```
Cisco Controller > config wlan security wpa osen enable 12
```

config wlan security wpa wpa1 disable

To disable WPA1, use the **config wlan security wpa wpa1 disable** command.

config wlan security wpa wpa1 disable *wlan_id*

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to disable WPA1:

```
(Cisco Controller) >config wlan security wpa wpa1 disable 1
```

config wlan security wpa wpa1 enable

To enable WPA1, use the **config wlan security wpa wpa1 enable** command.

config wlan security wpa wpa1 enable *wlan_id*

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable WPA1:

```
(Cisco Controller) >config wlan security wpa wpa1 enable 1
```

config wlan security wpa wpa2 disable

To disable WPA2, use the **config wlan security wpa wpa2 disable** command.

config wlan security wpa wpa2 disable *wlan_id*

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to disable WPA2:

```
(Cisco Controller) >config wlan security wpa wpa2 disable 1
```

config wlan security wpa wpa2 enable

To enable WPA2, use the **config wlan security wpa wpa2 enable** command.

config wlan security wpa wpa2 enable *wlan_id*

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable WPA2:

```
(Cisco Controller) >config wlan security wpa wpa2 enable 1
```

config wlan security wpa wpa2 cache

To configure caching methods on a WLAN, use the **config wlan security wpa wpa2 cache** command.

config wlan security wpa wpa2 cache sticky {**enable** | **disable**} *wlan_id*

Syntax Description

sticky	Configures Sticky Key Caching (SKC) roaming support on the WLAN.
enable	Enables SKC roaming support on the WLAN.
disable	Disables SKC roaming support on the WLAN.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

In SKC (Sticky Key caching) also known as PKC (Pro Active Key caching), the client stores each Pairwise Master Key (PMK) ID (PMKID) against a Pairwise Master Key Security Association (PMKSA). When a client finds an AP for which it has a PMKSA, it sends the PMKID in the association request to the AP. If the PMKSA is alive in the AP, the AP provides support for fast roaming. In SKC, full authentication is done on each new AP to which the client associates and the client must keep the PMKSA associated with all APs.

The following example shows how to enable SKC roaming support on a WLAN:

```
(Cisco Controller) >config wlan security wpa wpa2 cache sticky enable 1
```

config wlan security wpa wpa2 cache sticky

To configure Sticky PMKID Caching (SKC) on a WLAN, use the **config wlan security wpa wpa2 cache sticky** command.

config wlan security wpa wpa2 cache sticky {**enable** | **disable**} *wlan_id*

Syntax Description

enable	Enables SKC on a WLAN.
disable	Disables SKC on a WLAN.
wlan_id	Wireless LAN identifier between 1 and 512 (inclusive).

Command Default

Stkcky PMKID Caching is disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Beginning in Release 7.2 and later releases, the controller supports Sticky PMKID Caching (SKC). With sticky PMKID caching, the client receives and stores a different PMKID for every AP it associates with. The APs also maintain a database of the PMKID issued to the client. In SKC also known as PKC (Pro Active Key caching), the client stores each Pairwise Master Key (PMK) ID (PMKID) against a Pairwise Master Key Security Association (PMKSA). When a client finds an AP for which it has the PMKSA, it sends the PMKID in the association request to the AP. If the PMKSA is alive in the AP, the AP provides support for fast roaming. In SKC, full authentication is done on each new AP to which the client associates and the client must keep the PMKSA associated with all APs. For SKC, PMKSA is a per AP cache that the client stores and PMKSA is precalculated based on the BSSID of the new AP.

- You cannot use SKC for large scale deployments as the controller supports SKC only up to eight APs.
- SKC does not work across controllers in a mobility group.
- SKC works only on WPA2-enabled WLANs.
- SKC works only on local mode APs.

The following example shows how to enable Sticky PMKID Caching on WLAN 5:

```
(Cisco Controller) >config wlan security wpa wpa2 cache sticky enable 5
```

config wlan security wpa wpa2 ciphers

To configure WPA2 ciphers and enable or disable Advanced Encryption Standard (AES) or Temporal Key Integrity Protocol (TKIP) data encryption for WPA2, use the **config wlan security wpa wpa2 ciphers** command

config wlan security wpa wpa2 ciphers {**aes** | **tkip**} {**enable** | **disable**} *wlan_id*

Syntax Description

(Cisco Controller) > **aes**	Configures AES data encryption for WPA2.
tkip	Configures TKIP data encryption for WPA2.
enable	Enables AES or TKIP data encryption for WPA2.
disable	Disables AES or TKIP data encryption for WPA2.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

AES is enabled by default.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable AES data encryption for WPA2:

```
(Cisco Controller) >config wlan security wpa wpa2 ciphers aes enable 1
```

config wlan session-timeout

To change the timeout of wireless LAN clients, use the **config wlan session-timeout** command.

config wlan session-timeout {*wlan_id* | **foreignAp**} *seconds*

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.
seconds	Timeout or session duration in seconds. A value of zero is equivalent to no timeout. **Note** The range of session timeout depends on the security type: • Open system: 0-65535 (sec) • 802.1x: 300-86400 (sec) • static wep: 0-65535 (sec) • cranite: 0-65535 (sec) • fortress: 0-65535 (sec) • CKIP: 0-65535 (sec) • open+web auth: 0-65535 (sec) • web pass-thru: 0-65535 (sec) • wpa-psk: 0-65535 (sec) • disable: To disable reauth/session-timeout timers.

Command Default

None

Usage Guidelines

For 802.1X client security type, which creates the PMK cache, the maximum session timeout that can be set is 86400 seconds when the session timeout is disabled. For other client security such as open, WebAuth, and PSK for which the PMK cache is not created, the session timeout value is shown as infinite when session timeout is disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the client timeout to 6000 seconds for WLAN ID 1:

```
(Cisco Controller) >config wlan session-timeout 1 6000
```

config wlan sip-cac disassoc-client

To enable client disassociation in case of session initiation protocol (SIP) call admission control (CAC) failure, use the **config wlan sip-cac disassoc-client** command.

config wlan sip-cac disassoc-client {**enable** | **disable**} *wlan_id*

Syntax Description

enable	Enables a client disassociation on a SIP CAC failure.
disable	Disables a client disassociation on a SIP CAC failure.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

Client disassociation for SIP CAC is disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable a client disassociation on a SIP CAC failure where the WLAN ID is 1:

```
(Cisco Controller) >config wlan sip-cac disassoc-client enable 1
```

config wlan sip-cac send-486busy

To configure sending session initiation protocol (SIP) 486 busy message if a SIP call admission control (CAC) failure occurs, use the **config wlan sip-cac send-486busy** command:

config wlan sip-cac send-486busy {**enable** | **disable**} *wlan_id*

Syntax Description

enable	Enables sending a SIP 486 busy message upon a SIP CAC failure.
disable	Disables sending a SIP 486 busy message upon a SIP CAC failure.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

Session initiation protocol is enabled by default.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable sending a SIP 486 busy message upon a SIP CAC failure where the WLAN ID is 1:

```
(Cisco Controller) >config wlan sip-cac send-busy486 enable 1
```

config wlan ssid

To edit an SSID associated to a WLAN, use the **config wlan ssid** command.

config wlan ssid *wlan_id ssid*

Syntax Description

wlan_id	WLAN identifier from 1 to 512.
ssid	Service Set Identifier (SSID) associated to a WLAN.

Command Default

None

Command History

Release	Modification
8.0	This command was introduced.

The following example shows how to edit an SSID associated to a WLAN:

```
(Cisco Controller) >config wlan disable 1
(Cisco Controller) >config wlan ssid 1 new_samp
(Cisco Controller) >show wlan summary
Number of WLANs.................................. 1

WLAN ID  WLAN Profile Name / SSID   Status    Interface Name   PMIPv6 Mobility
-------  -------------------------  -------  ----------------  ---------------
1        sample / new_samp          Disabled   management            none
```

config wlan static-ip tunneling

To configure static IP client tunneling support on a WLAN, use the **config wlan static-ip tunneling** command.

config wlan static-ip tunneling {**enable** | **disable**} *wlan_id*

Syntax Description

tunneling	Configures static IP client tunneling support on a WLAN.
enable	Enables static IP client tunneling support on a WLAN.
disable	Disables static IP client tunneling support on a WLAN.
wlan_id	Wireless LAN identifier from 1 to 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable static IP client tunneling support for WLAN ID 3:

```
(Cisco Controller) >config wlan static-ip tunneling enable 34
```

config wlan uapsd compliant client enable

To enable WPA1, use the **config wlan uapsd compliant-client enable** command.

Note This was introduced for Ascom non-wmm capable phones and is not applicable for Cisco 792x/9971 IP phones.

config wlan uapsd compliant-client enable*wlan-id*

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable WPA1:

```
(Cisco Controller) >config wlan uapsd compliant-client enable 1
```

Property Type	Property Value	Property Description

config wlan uapsd compliant-client disable

To disable WPA1, use the **config wlan uapsd compliant-client disable** command.

Note This was introduced for Ascom non-wmm capable phones and is not applicable for Cisco 792x/9971 IP phones.

config wlan uapsd compliant-client disable*wlan-id*

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable WPA1:

```
(Cisco Controller) >config wlan uapsd compliant-client disable 1
```

config wlan url-acl

To configure the WLAN's URL ACL, use the **config wlan url-acl** command.

config wlan url-acl*WLAN-id acl-name*

Syntax Description

WLAN-id	WLAN Identifier. The range is between 1 and 512.
acl-name	Name of the ACL.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

This example shows how to cofigure a WLAN URL ACL:

```
(Cisco Controller) >config wlan url-acl 3 testacl
```

config wlan user-idle-threshold

To configure the threshold data sent by the client during the idle timeout for client sessions for a WLAN, use the **config wlan user-idle-threshold** command.

config wlan user-idle-threshold *bytes wlan_id*

Syntax Description

bytes	Threshold data sent by the client during the idle timeout for the client session for a WLAN. If the client send traffic less than the defined threshold, the client is removed on timeout. The range is from 0 to 10000000 bytes.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

The default timeout for threshold data sent by client during the idle timeout is 0 bytes.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the threshold data sent by the client during the idle timeout for client sessions for a WLAN:

```
(Cisco Controller) >config wlan user-idle-threshold 100 1
```

config wlan usertimeout

To configure the timeout for idle client sessions for a WLAN, use the **config wlan usertimeout** command.

config wlan usertimeout *timeout wlan_id*

Syntax Description

timeout	Timeout for idle client sessions for a WLAN. If the client sends traffic less than the threshold, the client is removed on timeout. The range is from 15 to 100000 seconds.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

The default client session idle timeout is 300 seconds.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

The timeout value that you configure here overrides the global timeout that you define using the command **config network usertimeout**.

The following example shows how to configure the idle client sessions for a WLAN:

```
(Cisco Controller) >config wlan usertimeout 100 1
```

config wlan webauth-exclude

To release the guest user IP address when the web authentication policy time expires and exclude the guest user from acquiring an IP address for three minutes, use the **config wlan webauth-exclude** command.

config wlan webauth-exclude *wlan_id* {**enable** | **disable**}

Syntax Description

wlan_id	Wireless LAN identifier (1 to 512).
enable	Enables web authentication exclusion.
disable	Disables web authentication exclusion.

Command Default

Disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

You can use this command for guest WLANs that are configured with web authentication.

This command is applicable when you configure the internal DHCP scope on the controller.

By default, when the web authentication timer expires for a guest user, the guest user can immediately reassociate with the same IP address before another guest user can acquire the IP address. If there are many guest users or limited IP address in the DHCP pool, some guest users might not be able to acquire an IP address.

When you enable this feature on the guest WLAN, the guest user's IP address is released when the web authentication policy time expires and the guest user is excluded from acquiring an IP address for three minutes. The IP address is available for another guest user to use. After three minutes, the excluded guest user can reassociate and acquire an IP address, if available.

The following example shows how to enable the web authentication exclusion for WLAN ID 5:

```
(Cisco Controller) >config wlan webauth-exclude 5 enable
```

config wlan wgb broadcast-tagging

To configure WGB broadcast tagging on a WLAN, use the **config wlan wgb broadcast-tagging** command.

config wlan wgb broadcast-tagging {**enable** | **disable**} *wlan-id*

Syntax Description

enable	Enables downlink broadcast packet VLAN tagging on a WLAN.
disable	Disables downlink broadcast packet VLAN tagging on a WLAN.
wlan-id	WLAN ID on which the configuration is to be applied.

Command Default

WGB broadcast tagging is disabled by default.

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to enable WGB broadcast tagging on WLAN ID 1:

```
(Cisco Controller) >config wlan wgb broadcast-tagging wlan 1
```

config wlan wifidirect

To configure Wi-Fi Direct Client Policy on a WLAN, use the **config wlan wifidirect** command.

config wlan wifidirect {**allow** | **disable** | **not-allow** | **xconnect-not-allow**} *wlan_id*

Syntax Description

allow	Allows Wi-Fi Direct clients to associate with the WLAN
disable	Ignores the Wi-Fi Direct status of clients thereby allowing Wi-Fi Direct clients to associate
not-allow	
xconnect-not-allow	Disallows the Wi-Fi Direct clients from associating with the WLAN
wlan_id	Wireless LAN identifier (1 to 16).

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to allow Wi-Fi Direct Client Policy on WLAN ID 1:

```
(Cisco Controller) >config wlan wifidirect allow 1
```

config wlan wmm

To configure Wi-Fi Multimedia (WMM) mode on a wireless LAN, use the **config wlan wmm** command.

config wlan wmm {**allow** | **disable** | **require**} *wlan_id*

Syntax Description

allow	Allows WMM on the wireless LAN.
disable	Disables WMM on the wireless LAN.
require	Specifies that clients use WMM on the specified wireless LAN.
wlan_id	Wireless LAN identifier (1 to 512).

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

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.

The following example shows how to configure wireless LAN ID 1 to allow WMM:

```
(Cisco Controller) >config wlan wmm allow 1
```

The following example shows how to configure wireless LAN ID 1 to specify that clients use WMM:

```
(Cisco Controller) >config wlan wmm require 1
```

config wps ap-authentication

To configure access point neighbor authentication, use the **config wps ap-authentication** command.

config wps ap-authentication [**enable** | **disable threshold** *threshold_value*]

Syntax Description

enable	(Optional) Enables WMM on the wireless LAN.
disable	(Optional) Disables WMM on the wireless LAN.
threshold	(Optional) Specifies that WMM-enabled clients are on the wireless LAN.
threshold_value	Threshold value (1 to 255).

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the access point neighbor authentication:

```
(Cisco Controller) > config wps ap-authentication threshold 25
```

Related Commands

show wps ap-authentication summary

config wps auto-immune

To enable or disable protection from Denial of Service (DoS) attacks, use the **config wps auto-immune** command.

config wps auto-immune {**enable** | **disable** | **stop**}

Syntax Description

enable	Enables the auto-immune feature.
disable	Disables the auto-immune feature.
stop	Stops dynamic auto-immune feature.

Command Default

Disabled

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

A potential attacker can use specially crafted packets to mislead the Intrusion Detection System (IDS) into treating a legitimate client as an attacker. It causes the controller to disconnect this legitimate client and launch a DoS attack. The auto-immune feature, when enabled, is designed to protect against such attacks. However, conversations using Cisco 792x phones might be interrupted intermittently when the auto-immune feature is enabled. If you experience frequent disruptions when using 792x phones, you might want to disable this feature.

The following example shows how to configure the auto-immune mode:

```
(Cisco Controller) > config wps auto-immune enable
```

The following example shows how to stop the auto-immune mode:

```
(Cisco Controller) > config wps auto-immune stop
Dynamic Auto Immune by WIPS is stopped
```

Related Commands

show wps summary

config wps cids-sensor

To configure Intrusion Detection System (IDS) sensors for the Wireless Protection System (WPS), use the **config wps cids-sensor** command.

config wps cids-sensor { [**add** *index ip_address username password*] | [**delete** *index*] | [**enable** *index*] | [**disable** *index*] | [**port** *index port*] | [**interval** *index query_interval*] | [**fingerprint sha1** *fingerprint*] }

Syntax Description

add	(Optional) Configures a new IDS sensor.
index	IDS sensor internal index.
ip_address	IDS sensor IP address.
username	IDS sensor username.
password	IDS sensor password.
delete	(Optional) Deletes an IDS sensor.
enable	(Optional) Enables an IDS sensor.
disable	(Optional) Disables an IDS sensor.
port	(Optional) Configures the IDS sensor's port number.
port	Port number.
interval	(Optional) Specifies the IDS sensor's query interval.
query_interval	Query interval setting.
fingerprint	(Optional) Specifies the IDS sensor's TLS fingerprint.
sha1	(Optional) Specifies the TLS fingerprint.
fingerprint	TLS fingerprint.

Command Default

Command defaults are listed below as follows:

Port	443
Query interval	60
Certification fingerprint	00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
Query state	Disabled

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the intrusion detection system with the IDS index 1, IDS sensor IP address 10.0.0.51, IDS username Sensor_user0doc1, and IDS password passowrd01:

```
(Cisco Controller) > config wps cids-sensor add 1 10.0.0.51 Sensor_user0doc1 password01
```

Related Commands

show wps cids-sensor detail

config wps client-exclusion

To configure client exclusion policies, use the **config wps client-exclusion** command.

config wps client-exclusion {**802.11-assoc** | **802.11-auth** | **802.11x-auth** | **ip-theft** | **web-auth** | **all**} {**enable** | **disable**}

Syntax Description

802.11-assoc	Specifies that the controller excludes clients on the sixth 802.11 association attempt, after five consecutive failures.
802.11-auth	Specifies that the controller excludes clients on the sixth 802.11 authentication attempt, after five consecutive failures.
802.1x-auth	Specifies that the controller excludes clients on the sixth 802.11X authentication attempt, after five consecutive failures.
ip-theft	Specifies that the control excludes clients if the IP address is already assigned to another device.
web-auth	Specifies that the controller excludes clients on the fourth web authentication attempt, after three consecutive failures.
all	Specifies that the controller excludes clients for all of the above reasons.
enable	Enables client exclusion policies.
disable	Disables client exclusion policies.

Command Default

All policies are enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to disable clients on the 802.11 association attempt after five consecutive failures:

```
(Cisco Controller) > config wps client-exclusion 802.11-assoc disable
```

Related Commands

show wps summary

config wps mfp

To configure Management Frame Protection (MFP), use the **config wps mfp** command.

config wps mfp {**infrastructure** | **ap-impersonation**} {**enable** | **disable**}

Syntax Description

infrastructure	Configures the MFP infrastructure.
ap-impersonation	Configures ap impersonation detection by MFP.
enable	Enables the MFP feature.
disable	Disables the MFP feature.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the infrastructure MFP:

```
(Cisco Controller) > config wps mfp infrastructure enable
```

Related Commands

show wps mfp

config wps shun-list re-sync

To force the controller to synchronization with other controllers in the mobility group for the shun list, use the **config wps shun-list re-sync** command.

config wps shun-list re-sync

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the controller to synchronize with other controllers for the shun list:

```
(Cisco Controller) > config wps shun-list re-sync
```

Related Commands

show wps shun-list

config wps signature

To enable or disable Intrusion Detection System (IDS) signature processing, or to enable or disable a specific IDS signature, use the **config wps signature** command.

config wps signature {**standard** | **custom**} **state** *signature_id* {**enable** | **disable**}

Syntax Description

standard	Configures a standard IDS signature.
custom	Configures a standard IDS signature.
state	Specifies the state of the IDS signature.
signature_id	Identifier for the signature to be enabled or disabled.
enable	Enables the IDS signature processing or a specific IDS signature.
disable	Disables IDS signature processing or a specific IDS signature.

Command Default

IDS signature processing is enabled by default.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

If IDS signature processing is disabled, all signatures are disabled, regardless of the state configured for individual signatures.

The following example shows how to enable IDS signature processing, which enables the processing of all IDS signatures:

```
(Cisco Controller) >config wps signature enable
```

The following example shows how to disable a standard individual IDS signature:

```
(Cisco Controller) > config wps signature standard state 15 disable
```

Related Commands

config wps signature frequency

config wps signature interval

config wps signature mac-frequency

config wps signature quiet-time

config wps signature reset

show wps signature events

show wps signature summary

show wps summary

config wps signature frequency

To specify the number of matching packets per interval that must be identified at the individual access point level before an attack is detected, use the **config wps signature frequency** command.

config wps signature frequency *signature_id frequency*

Syntax Description

signature_id	Identifier for the signature to be configured.
frequency	Number of matching packets per interval that must be at the individual access point level before an attack is detected. The range is 1 to 32,000 packets per interval.

Command Default

The *frequency* default value varies per signature.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

If IDS signature processing is disabled, all signatures are disabled, regardless of the state configured for individual signatures.

The following example shows how to set the number of matching packets per interval per access point before an attack is detected to 1800 for signature ID 4:

```
(Cisco Controller) > config wps signature frequency 4 1800
```

Related Commands

config wps signature frequency

config wps signature interval

config wps signature quiet-time

config wps signature reset

show wps signature events

show wps signature summary

show wps summary

config wps signature interval

To specify the number of seconds that must elapse before the signature frequency threshold is reached within the configured interval, use the **config wps signature interval** command.

config wps signature interval *signature_id interval*

Syntax Description

signature_id	Identifier for the signature to be configured.
interval	Number of seconds that must elapse before the signature frequency threshold is reached. The range is 1 to 3,600 seconds.

Command Default

The default value of *interval* varies per signature.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

If IDS signature processing is disabled, all signatures are disabled, regardless of the state configured for individual signatures.

The following example shows how to set the number of seconds to elapse before reaching the signature frequency threshold to 200 for signature ID 1:

```
(Cisco Controller) > config wps signature interval 1 200
```

Related Commands

config wps signature frequency

config wps signature

config wps signature mac-frequency

config wps signature quiet-time

config wps signature reset

show wps signature events

show wps signature summary

show wps summary

config wps signature mac-frequency

To specify the number of matching packets per interval that must be identified per client per access point before an attack is detected, use the **config wps signature mac-frequency** command.

config wps signature mac-frequency *signature_id mac_frequency*

Syntax Description

signature_id	Identifier for the signature to be configured.
mac_frequency	Number of matching packets per interval that must be identified per client per access point before an attack is detected. The range is 1 to 32,000 packets per interval.

Command Default

The *mac_frequency* default value varies per signature.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

If IDS signature processing is disabled, all signatures are disabled, regardless of the state configured for individual signatures.

The following example shows how to set the number of matching packets per interval per client before an attack is detected to 50 for signature ID 3:

```
(Cisco Controller) > config wps signature mac-frequency 3 50
```

Related Commands

config wps signature frequency

config wps signature interval

config wps signature

config wps signature quiet-time

config wps signature reset

show wps signature events

show wps signature summary

show wps summary

config wps signature quiet-time

To specify the length of time after which no attacks have been detected at the individual access point level and the alarm can stop, use the **config wps signature quiet-time** command.

config wps signature quiet-time *signature_id quiet_time*

Syntax Description

signature_id	Identifier for the signature to be configured.
quiet_time	Length of time after which no attacks have been detected at the individual access point level and the alarm can stop. The range is 60 to 32,000 seconds.

Command Default

The default value of *quiet_time* varies per signature.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

If IDS signature processing is disabled, all signatures are disabled, regardless of the state configured for individual signatures.

The following example shows how to set the number of seconds after which no attacks have been detected per access point to 60 for signature ID 1:

```
(Cisco Controller) > config wps signature quiet-time 1 60
```

Related Commands

config wps signature

config wps signature frequency

config wps signature interval

config wps signature mac-frequency

config wps signature reset

show wps signature events

show wps signature summary

show wps summary

config wps signature reset

To reset a specific Intrusion Detection System (IDS) signature or all IDS signatures to default values, use the **config wps signature reset** command.

config wps signature reset {*signature_id* | **all**}

Syntax Description

signature_id	Identifier for the specific IDS signature to be reset.
all	Resets all IDS signatures.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

If IDS signature processing is disabled, all signatures are disabled, regardless of the state configured for individual signatures.

The following example shows how to reset the IDS signature 1 to default values:

```
(Cisco Controller) > config wps signature reset 1
```

Related Commands

config wps signature

config wps signature frequency

config wps signature interval

config wps signature mac-frequency

config wps signature quiet-time

show wps signature events

show wps signature summary

show wps summary