Security Commands

- clear acl counters, on page 6
- clear radius acct statistics, on page 7
- clear tacacs auth statistics, on page 8
- clear stats local-auth, on page 9
- clear stats radius, on page 10
- clear stats tacacs, on page 11
- config 802.11b preamble, on page 12
- config aaa auth, on page 13
- config aaa auth mgmt, on page 14
- config acl apply, on page 15
- config acl counter, on page 16
- config acl create, on page 17
- config acl cpu, on page 18
- config acl delete, on page 19
- config acl layer2, on page 20
- config acl rule, on page 22
- config auth-list add, on page 24
- config auth-list ap-policy, on page 25
- config auth-list delete, on page 26
- config advanced eap, on page 27
- config advanced timers auth-timeout, on page 29
- config advanced timers eap-timeout, on page 30
- config advanced timers eap-identity-request-delay, on page 31
- config cts sxp, on page 32
- config database size, on page 33
- config dhcp opt-82 format, on page 34
- config dhcp opt-82 remote-id, on page 35
- config exclusionlist, on page 36
- config ldap, on page 37
- config local-auth active-timeout, on page 39
- config local-auth eap-profile, on page 40
- config local-auth method fast, on page 42
- config local-auth user-credentials, on page 44

- config ipv6 acl, on page 45
- config netuser add , on page 47
- config netuser delete, on page 49
- config netuser description, on page 50
- config network bridging-shared-secret, on page 51
- config network web-auth captive-bypass, on page 52
- config network web-auth port, on page 53
- config network web-auth proxy-redirect, on page 54
- config network web-auth secureweb, on page 55
- config network webmode, on page 56
- config network web-auth, on page 57
- config policy, on page 58
- config radius acct, on page 61
- config radius acct ipsec authentication, on page 64
- config radius acct ipsec disable, on page 65
- config radius acct ipsec enable, on page 66
- config radius acct ipsec encryption, on page 67
- config radius acct ipsec ike, on page 68
- config radius acct mac-delimiter, on page 69
- config radius acct network, on page 70
- config radius acct retransmit-timeout, on page 71
- config radius auth, on page 72
- config radius auth callStationIdType, on page 74
- config radius auth IPsec authentication, on page 76
- config radius auth ipsec disable, on page 77
- config radius auth ipsec encryption, on page 78
- config radius auth ipsec ike, on page 79
- config radius auth keywrap, on page 81
- config radius auth mac-delimiter, on page 82
- config radius auth management, on page 83
- config radius auth mgmt-retransmit-timeout, on page 84
- config radius auth network, on page 85
- config radius auth retransmit-timeout, on page 86
- config radius auth rfc3576, on page 87
- config radius auth retransmit-timeout, on page 88
- config radius aggressive-failover disabled, on page 89
- config radius backward compatibility, on page 90
- config radius callStationIdCase, on page 91
- config radius callStationIdType, on page 92
- config radius dns, on page 94
- config radius fallback-test, on page 96
- config rogue adhoc, on page 98
- config rogue ap classify, on page 101
- config rogue ap friendly, on page 103
- config rogue ap rldp, on page 105
- config rogue ap ssid, on page 107

- config rogue ap timeout, on page 109
- config rogue auto-contain level, on page 110
- config rogue ap valid-client, on page 112
- config rogue client, on page 114
- config rogue containment, on page 116
- config rogue detection, on page 117
- config rogue detection client-threshold, on page 118
- config rogue detection min-rssi, on page 119
- config rogue detection monitor-ap, on page 120
- config rogue detection report-interval, on page 122
- config rogue detection security-level, on page 123
- config rogue detection transient-rogue-interval, on page 124
- config rogue rule, on page 125
- config rogue rule condition ap, on page 129
- config tacacs acct, on page 131
- config tacacs athr, on page 133
- config tacacs athr mgmt-server-timeout, on page 135
- config tacacs auth, on page 136
- config tacacs auth mgmt-server-timeout, on page 138
- config tacacs dns, on page 139
- config wps ap-authentication, on page 141
- config wps auto-immune, on page 142
- config wps cids-sensor, on page 143
- config wps client-exclusion, on page 145
- config wps mfp, on page 146
- config wps shun-list re-sync, on page 147
- config wps signature, on page 148
- config wps signature frequency, on page 150
- config wps signature interval, on page 151
- config wps signature mac-frequency, on page 152
- config wps signature quiet-time, on page 153
- config wps signature reset, on page 154
- debug 11w-pmf, on page 155
- debug aaa, on page 156
- debug aaa local-auth, on page 157
- debug bcast, on page 159
- debug cckm, on page 160
- debug cts sxp, on page 161
- debug dns, on page 162
- debug dot1x, on page 163
- debug dtls, on page 164
- debug nac, on page 165
- debug policy, on page 166
- debug pm, on page 167
- debug web-auth, on page 169
- debug wips, on page 170

- debug wps sig, on page 171
- debug wps mfp, on page 172
- show 802.11, on page 173
- show aaa auth, on page 175
- show acl, on page 176
- show advanced eap, on page 178
- show database summary, on page 179
- show exclusionlist, on page 180
- show ike, on page 181
- show IPsec, on page 182
- show ipv6 acl, on page 184
- show ipv6 summary, on page 185
- show l2tp, on page 186
- show ldap, on page 187
- show ldap statistics, on page 188
- show ldap summary, on page 189
- show local-auth certificates, on page 190
- show local-auth config, on page 191
- show local-auth statistics, on page 193
- show nac statistics, on page 195
- show nac summary, on page 196
- show netuser, on page 197
- show netuser guest-roles, on page 198
- show network, on page 199
- show network summary, on page 200
- show ntp-keys, on page 202
- show policy, on page 203
- show profiling policy summary, on page 205
- show radius acct statistics, on page 208
- show radius auth statistics, on page 209
- show radius summary, on page 210
- show rules, on page 211
- show switchconfig, on page 212
- show rogue adhoc custom summary, on page 213
- show rogue adhoc detailed, on page 214
- show rogue adhoc friendly summary , on page 215
- show rogue adhoc malicious summary, on page 216
- show rogue adhoc unclassified summary , on page 217
- show rogue adhoc summary, on page 218
- show rogue ap custom summary , on page 219
- show rogue ap clients, on page 221
- show rogue ap detailed, on page 223
- show rogue ap summary, on page 226
- show rogue ap friendly summary, on page 229
- show rogue ap malicious summary, on page 231
- show rogue ap unclassified summary, on page 233

- show rogue auto-contain, on page 234
- show rogue client detailed, on page 235
- show rogue client summary, on page 236
- show rogue ignore-list, on page 237
- show rogue rule detailed, on page 239
- show rogue rule summary, on page 241
- show tacacs acct statistics, on page 242
- show tacacs athr statistics, on page 243
- show tacacs auth statistics, on page 244
- show tacacs summary, on page 245
- show wps ap-authentication summary, on page 246
- show wps cids-sensor, on page 247
- show wps mfp, on page 248
- show wps shun-list, on page 249
- show wps signature detail, on page 250
- show wps signature events, on page 251
- show wps signature summary, on page 253
- show wps summary, on page 255
- show wps wips statistics, on page 257
- show wps wips summary, on page 258

clear acl counters

To clear the current counters for an Access Control List (ACL), use the **clear acl counters** command.

clear acl counters *acl_name*

Syntax Description

acl_name	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 clear the current counters for acl1:

```
(Cisco Controller) >clear acl counters acl1
```

clear radius acct statistics

To clear the RADIUS accounting statistics on the controller, use the **clear radius acc statistics** command.

clear radius acct statistics [**index** | **all**]

Syntax Description

index	(Optional) Specifies the index of the RADIUS accounting server.
all	(Optional) Specifies all RADIUS accounting 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 clear the RADIUS accounting statistics:

```
(Cisco Controller) >clear radius acc statistics
```

Related Commands

show radius acct statistics

clear tacacs auth statistics

To clear the RADIUS authentication server statistics in the controller, use the **clear tacacs auth statistics** command.

clear tacacs auth statistics [**index** | **all**]

Syntax Description

index	(Optional) Specifies the index of the RADIUS authentication server.
all	(Optional) Specifies all RADIUS authentication 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 clear the RADIUS authentication server statistics:

```
(Cisco Controller) >clear tacacs auth statistics
```

Related Commands

show tacacs auth statistics

show tacacs summary

config tacacs auth

clear stats local-auth

To clear the local Extensible Authentication Protocol (EAP) statistics, use the **clear stats local-auth** command.

clear stats local-auth

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 clear the local EAP statistics:

```
(Cisco Controller) >clear stats local-auth
Local EAP Authentication Stats Cleared.
```

Related Commands

config local-auth active-timeout

config local-auth eap-profile

config local-auth method fast

config local-auth user-credentials

debug aaa local-auth

show local-auth certificates

show local-auth config

show local-auth statistics

clear stats radius

To clear the statistics for one or more RADIUS servers, use the **clear stats radius** command.

clear stats radius {**auth** | **acct**} {**index** | **all**}

Syntax Description

auth	Clears statistics regarding authentication.
acct	Clears statistics regarding accounting.
index	Specifies the index number of the RADIUS server to be cleared.
all	Clears statistics for all 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 clear the statistics for all RADIUS authentication servers:

```
(Cisco Controller) >clear stats radius auth all
```

Related Commands

clear transfer

clear download datatype

clear download filename

clear download mode

clear download serverip

clear download start

clear upload datatype

clear upload filename

clear upload mode

clear upload path

clear upload serverip

clear upload start

clear stats port

clear stats tacacs

To clear the TACACS+ server statistics on the controller, use the **clear stats tacacs** command.

clear stats tacacs [**auth** | **athr** | **acct**] [**index** | **all**]

Syntax Description

auth	(Optional) Clears the TACACS+ authentication server statistics.
athr	(Optional) Clears the TACACS+ authorization server statistics.
acct	(Optional) Clears the TACACS+ accounting server statistics.
index	(Optional) Specifies index of the TACACS+ server.
all	(Optional) Specifies all TACACS+ 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 clear the TACACS+ accounting server statistics for index 1:

```
(Cisco Controller) >clear stats tacacs acct 1
```

Related Commands

show tacacs summary

config 802.11b preamble

To change the 802.11b preamble as defined in subclause 18.2.2.2 to **long** (slower, but more reliable) or **short** (faster, but less reliable), use the **config 802.11b preamble** command.

config 802.11b preamble {**long** | **short**}

Syntax Description

long	Specifies the long 802.11b preamble.
short	Specifies the short 802.11b preamble.

Command Default

The default 802.11b preamble value is short.

Command History

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

Usage Guidelines

Note You must reboot the Cisco Wireless LAN Controller (reset system) with save to implement this command.

This parameter must be set to **long** to optimize this Cisco wireless LAN controller for some clients, including SpectraLink NetLink telephones.

This command can be used any time that the CLI interface is active.

The following example shows how to change the 802.11b preamble to short:

```
(Cisco Controller) >config 802.11b preamble short
(Cisco Controller) >(reset system with save)
```

config aaa auth

To configure the AAA authentication search order for management users, use the **config aaa auth** command.

config aaa auth mgmt [*aaa_server_type1* | *aaa_server_type2*]

Syntax Description

mgmt	Configures the AAA authentication search order for controller management users by specifying up to three AAA authentication server types. The order that the server types are entered specifies the AAA authentication search order.
aaa_server_type	(Optional) AAA authentication server type (**local**, **radius**, or **tacacs**). The **local** setting specifies the local database, the **radius** setting specifies the RADIUS server, and the **tacacs** setting specifies the TACACS+ server.

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 enter two AAA server types as long as one of the server types is **local**. You cannot enter **radius** and **tacacs** together.

The following example shows how to configure the AAA authentication search order for controller management users by the authentication server type local:

```
(Cisco Controller) > config aaa auth radius local
```

Related Commands

show aaa auth

config aaa auth mgmt

To configure the order of authentication when multiple databases are configured, use the **config aaa auth mgmt** command.

config aaa auth mgmt [**radius** | **tacacs**]

Syntax Description

radius	(Optional) Configures the order of authentication for RADIUS servers.
tacacs	(Optional) Configures the order of authentication for TACACS 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 configure the order of authentication for the RADIUS server:

```
(Cisco Controller) > config aaa auth mgmt radius
```

The following example shows how to configure the order of authentication for the TACACS server:

```
(Cisco Controller) > config aaa auth mgmt tacacs
```

Related Commands

show aaa auth order

config acl apply

To apply an access control list (ACL) to the data path, use the **config acl apply** command.

config acl apply *rule_name*

Syntax Description

rule_name	ACL name that contains 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.

Example

The following example shows how to apply an ACL to the data path:

```
(Cisco Controller) > config acl apply acl01
```

config acl counter

To see if packets are hitting any of the access control lists (ACLs) configured on your controller, use the **config acl counter** command.

config acl counter {**start** | **stop**}

Syntax Description

start	Enables ACL counters on your controller.
stop	Disables ACL counters on your controller.

Command Default

None

Command History

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

Usage Guidelines

ACL counters are available only on the following controllers: 4400 series, Cisco WiSM, and Catalyst 3750G Integrated Wireless LAN Controller Switch.

The following example shows how to enable ACL counters on your controller:

```
(Cisco Controller) > config acl counter start
```

Related Commands

clear acl counters

show acl detailed

config acl create

To create a new access control list (ACL), use the **config acl create** command.

config acl create *rule_name*

Syntax Description

rule_name	ACL name that contains 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.

Usage Guidelines

For a Cisco 2100 Series Wireless LAN Controller, you must configure a preauthentication ACL on the wireless LAN for the external web server. This ACL should then be set as a wireless LAN preauthentication ACL under Web Policy. However, you do not need to configure any preauthentication ACL for Cisco 4400 Series Wireless LAN Controllers.

The following example shows how to create a new ACL:

```
(Cisco Controller) > config acl create acl01
```

Related Commands

show acl

config acl cpu

To create a new access control list (ACL) rule that restricts the traffic reaching the CPU, use the **config acl cpu** command.

config acl cpu *rule_name* {**wired** | **wireless** | **both**}

Syntax Description

rule_name	Specifies the ACL name.
wired	Specifies an ACL on wired traffic.
wireless	Specifies an ACL on wireless traffic.
both	Specifies an ACL on both wired and wireless traffic.

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 allows you to control the type of packets reaching the CPU.

The following example shows how to create an ACL named acl101 on the CPU and apply it to wired traffic:

```
(Cisco Controller) > config acl cpu acl01 wired
```

Related Commands

show acl cpu

config acl delete

To delete an access control list (ACL), use the **config acl delete** command.

config acl delete *rule_name*

Syntax Description

rule_name	ACL name that contains 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.

Usage Guidelines

For a Cisco 2100 Series Wireless LAN Controller, you must configure a preauthentication ACL on the wireless LAN for the external web server. This ACL should then be set as a wireless LAN preauthentication ACL under Web Policy. However, you do not need to configure any preauthentication ACL for Cisco 4400 Series Wireless LAN Controllers.

The following example shows how to delete an ACL named acl101 on the CPU:

```
(Cisco Controller) > config acl delete acl01
```

Related Commands

show acl

config acl layer2

To configure a Layer 2 access control list (ACL), use the **config acl layer2** command.

config acl layer2 {**apply** *acl_name* | **create** *acl_name* | **delete** *acl_name* | **rule** {**action** *acl_name index* {**permit** | **deny**} | **add** *acl_name index* | **change index** *acl_name old_index new_index* | **delete** *acl_name index* | **etherType** *acl_name index etherType etherTypeMask* | **swap index** *acl_name index1 index2*}}

Syntax Description

apply	Applies a Layer 2 ACL to the data path.
acl_name	Layer 2 ACL name. The name can be up to 32 alphanumeric characters.
create	Creates a Layer 2 ACL.
delete	Deletes a Layer 2 ACL.
rule	Configures a Layer 2 ACL rule.
action	Configures the action for the Layer 2 ACL rule.
index	Index of the Layer 2 ACL rule.
permit	Permits rule action.
deny	Denies rule action.
add	Creates a Layer 2 ACL rule.
change index	Changes the index of the Layer 2 ACL rule.
old_index	Old index of the Layer 2 ACL rule.
new_index	New index of the Layer 2 ACL rule.
delete	Deletes a Layer 2 ACL rule.
etherType	Configures the EtherType of a Layer 2 ACL rule.
etherType	EtherType of a Layer 2 ACL rule. EtherType is used to indicate the protocol that is encapsulated in the payload of an Ethernet frame. The range is a hexadecimal value from 0x0 to 0xffff.
etherTypeMask	Netmask of the EtherType. The range is a hexadecimal value from 0x0 to 0xffff.
swap index	Swaps the index values of two rules.
index1 index2	Index values of two Layer 2 ACL rules.

Command Default

The Cisco WLC does not have any Layer2 ACLs.

Command History

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

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:

```
(Cisco Controller) >config acl layer2 apply acl_l2_1
```

Related Topics

config acl counter, on page 16
config ap flexconnect wlan
config wlan layer2 acl
show acl, on page 176
show client detail
show wlan

config acl rule

To configure ACL rules, use the **config acl rule** command.

config acl rule {**action** *rule_name rule_index* {**permit** | **deny**} | **add** *rule_name rule_index* | **change index** *rule_name old_index new_index* | **delete** *rule_name rule_index* | **destination address** *rule_name rule_index ip_address netmask* | **destination port range** *rule_name rule_index start_port end_port* | **direction** *rule_name rule_index* {**in** | **out** | **any**} | **dscp** *rule_name rule_index dscp* | **protocol** *rule_name rule_index protocol* | **source address** *rule_name rule_index ip_address netmask* | **source port range** *rule_name rule_index start_port end_port* | **swap index** *rule_name index_1 index_2*}

Syntax Description

action	Configures whether to permit or deny access.
rule_name	ACL name that contains up to 32 alphanumeric characters.
rule_index	Rule index between 1 and 32.
permit	Permits the rule action.
deny	Denies the rule action.
add	Adds a new rule.
change	Changes a rule's index.
index	Specifies a rule index.
delete	Deletes a rule.
destination address	Configures a rule's destination IP address and netmask.
destination port range	Configure a rule's destination port range.
ip_address	IP address of the rule.
netmask	Netmask of the rule.
start_port	Start port number (between 0 and 65535).
end_port	End port number (between 0 and 65535).
direction	Configures a rule's direction to in, out, or any.
in	Configures a rule's direction to in.
out	Configures a rule's direction to out.
any	Configures a rule's direction to any.
dscp	Configures a rule's DSCP.

dscp	Number between 0 and 63, or **any**.
protocol	Configures a rule's DSCP.
protocol	Number between 0 and 255, or **any**.
source address	Configures a rule's source IP address and netmask.
source port range	Configures a rule's source port range.
swap	Swaps two rules' indices.

Command Default

None

Command History

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

Usage Guidelines

For a Cisco 2100 Series Wireless LAN Controller, you must configure a preauthentication ACL on the wireless LAN for the external web server. This ACL should then be set as a wireless LAN pre-authentication ACL under Web Policy. However, you do not need to configure any preauthentication ACL for Cisco 4400 Series Wireless LAN Controllers.

The following example shows how to configure an ACL to permit access:

```
(Cisco Controller) > config acl rule action lab1 4 permit
```

Related Commands

show acl

config auth-list add

To create an authorized access point entry, use the **config auth-list add** command.

config auth-list add {**mic** | **ssc**} *AP_MAC* [*AP_key*]

Syntax Description

mic	Specifies that the access point has a manufacture-installed certificate.
ssc	Specifies that the access point has a self-signed certificate.
AP_MAC	MAC address of a Cisco lightweight access point.
AP_key	(Optional) Key hash value that is equal to 20 bytes or 40 digits.

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 an authorized access point entry with a manufacturer-installed certificate on MAC address 00:0b:85:02:0d:20:

```
(Cisco Controller) > config auth-list add 00:0b:85:02:0d:20
```

Related Commands

config auth-list delete

config auth-list ap-policy

config auth-list ap-policy

To configure an access point authorization policy, use the **config auth-list ap-policy** command.

config auth-list ap-policy {**authorize-ap** {**enable** | **disable**} | **ssc** {**enable** | **disable**}}

Syntax Description

authorize-ap enable	Enables the authorization policy.
authorize-ap disable	Disables the AP authorization policy.
ssc enable	Allows the APs with self-signed certificates to connect.
ssc disable	Disallows the APs with self-signed certificates to connect.

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 access point authorization policy:

```
(Cisco Controller) > config auth-list ap-policy authorize-ap enable
```

The following example shows how to enable an access point with a self-signed certificate to connect:

```
(Cisco Controller) > config auth-list ap-policy ssc disable
```

Related Commands

config auth-list delete

config auth-list add

config auth-list delete

To delete an access point entry, use the **config auth-list delete** command.

config auth-list delete *AP_MAC*

Syntax Description

AP_MAC	MAC address of a Cisco lightweight access point.

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 access point entry for MAC address 00:1f:ca:cf:b6:60:

```
(Cisco Controller) > config auth-list delete 00:1f:ca:cf:b6:60
```

Related Commands

config auth-list delete

config auth-list add

config auth-list ap-policy

config advanced eap

To configure advanced extensible authentication protocol (EAP) settings, use the **config advanced eap** command.

config advanced eap {**bcast-key-interval** *seconds* | **eapol-key-timeout** *timeout* | **eapol-key-retries** *retries* | **identity-request-timeout** *timeout* | **identity-request-retries** *retries* | **key-index** *index* | **max-login-ignore-identity-response** {**enable** | **disable**} **request-timeout** *timeout* | **request-retries** *retries*} }

Syntax Description

bcast-key-interval *seconds*	Specifies the EAP-broadcast key renew interval time in seconds. The range is from 120 to 86400 seconds.
eapol-key-timeout *timeout*	Specifies the amount of time (200 to 5000 milliseconds) that the controller waits before retransmitting an EAPOL (WPA) key message to a wireless client using EAP or WPA/WPA-2 PSK. The default value is 1000 milliseconds.
eapol-key-retries *retries*	Specifies the maximum number of times (0 to 4 retries) that the controller retransmits an EAPOL (WPA) key message to a wireless client. The default value is 2.
identity-request- timeout *timeout*	Specifies the amount of time (1 to 120 seconds) that the controller waits before retransmitting an EAP Identity Request message to a wireless client. The default value is 30 seconds.
identity-request- retries	Specifies the maximum number of times (0 to 4 retries) that the controller retransmits an EAPOL (WPA) key message to a wireless client. The default value is 2.
key-index *index*	Specifies the key index (0 or 3) used for dynamic wired equivalent privacy (WEP).

max-login-ignore- identity-response	When enabled, this command ignores the limit set for the number of devices that can be connected to the controller with the same username using 802.1xauthentication. When disabled, this command limits the number of devices that can be connected to the controller with the same username. This option is not applicable for Web auth user. Use the command **config netuser maxUserLogin** to set the limit of maximum number of devices per same username
enable	Ignores the same username reaching the maximum EAP identity response.
disable	Checks the same username reaching the maximum EAP identity response.
request-timeout	For EAP messages other than Identity Requests or EAPOL (WPA) key messages, specifies the amount of time (1 to 120 seconds) that the controller waits before retransmitting the message to a wireless client. The default value is 30 seconds.
request-retries	(Optional) For EAP messages other than Identity Requests or EAPOL (WPA) key messages, specifies the maximum number of times (0 to 20 retries) that the controller retransmits the message to a wireless client. The default value is 2.

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 key index used for dynamic wired equivalent privacy (WEP):

```
(Cisco Controller) > config advanced eap key-index 0
```

config advanced timers auth-timeout

To configure the authentication timeout, use the **config advanced timers auth-timeout** command.

config advanced timers auth-timeout *seconds*

Syntax Description

seconds	Authentication response timeout value in seconds between 10 and 600.

Command Default

The default authentication timeout value is 10 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 the authentication timeout to 20 seconds:

```
(Cisco Controller) >config advanced timers auth-timeout 20
```

config advanced timers eap-timeout

To configure the Extensible Authentication Protocol (EAP) expiration timeout, use the **config advanced timers eap-timeout** command.

config advanced timers eap-timeout *seconds*

Syntax Description

seconds	EAP timeout value in seconds between 8 and 120.

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 EAP expiration timeout to 10 seconds:

```
(Cisco Controller) >config advanced timers eap-timeout 10
```

config advanced timers eap-identity-request-delay

To configure the advanced Extensible Authentication Protocol (EAP) identity request delay in seconds, use the **config advanced timers eap-identity-request-delay** command.

config advanced timers eap-identity-request-delay *seconds*

Syntax Description

seconds	Advanced EAP identity request delay in number of seconds between 0 and 10.

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 advanced EAP identity request delay to 8 seconds:

```
(Cisco Controller) >config advanced timers eap-identity-request-delay 8
```

config cts sxp

To configure Cisco TrustSec SXP (CTS) connections on the controller, use the **config cts sxp** command.

config cts sxp {**enable** | **disable** | **connection** {**delete** | **peer**} | **default password** *password* | **retry period** *time-in-seconds*}

Syntax Description

enable	Enables CTS connections on the controller.
disable	Disables CTS connections on the controller.
connection	Configures CTS connection on the controller.
delete	Deletes the CTS connection on the controller.
peer	Configures the next hop switch with which the controller is connected.
ip-address	Only IPv4 address of the peer.
default password	Configures the default password for MD5 authentication of SXP messages.
password	Default password for MD5 Authentication of SXP messages. The password should contain a minimum of six characters.
retry period	Configures the SXP retry period.
time-in-seconds	Time after which a CTS connection should be again tried for after a failure to connect.

Command Default

None

Command History

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

Usage Guidelines

For release 8.0, only IPv4 is supported for TrustSec SXP configuration.

The following example shows how to enable CTS on the controller:

```
(Cisco Controller) > config cts sxp enable
```

The following example shows how to configure a peer for a CTS connection:

```
> config cts sxp connection peer 209.165.200.224
```

Related Commands

debug cts sxp

config database size

To configure the local database, use the **config database size** command.

config database size *count*

Syntax Description

count	Database size value between 512 and 2040

Command Default

None

Command History

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

Usage Guidelines

Use the **show database** command to display local database configuration.

The following example shows how to configure the size of the local database:

```
(Cisco Controller) > config database size 1024
```

Related Commands

show database

config dhcp opt-82 format

To configure the DHCP option 82 format, use the **config dhcp opt-82 format** command.

config dhcp opt-82 format {*binary* | *ascii*}

Syntax Description

binary	Specifies the DHCP option 82 format as binary.
ascii	Specifies the DHCP option 82 format as ASCII.

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 format of DHCP option 82 payload:

```
(Cisco Controller) > config dhcp opt-82 format binary
```

config dhcp opt-82 remote-id

To configure the format of the DHCP option 82 payload, use the **config dhcp opt-82 remote-id** command.

config dhcp opt-82 remote-id {*ap_mac* | *ap_mac:ssid* | *ap-ethmac* | *apname:ssid* | *ap-group-name* | *flex-group-name* | *ap-location* | *apmac-vlan-id* | *apname-vlan-id* | *ap-ethmac-ssid*}

Syntax Description

ap_mac	Specifies the radio MAC address of the access point to the DHCP option 82 payload.
ap_mac:ssid	Specifies the radio MAC address and SSID of the access point to the DHCP option 82 payload.
ap-ethmac	Specifies the Ethernet MAC address of the access point to the DHCP option 82 payload.
apname:ssid	Specifies the AP name and SSID of the access point to the DHCP option 82 payload.
ap-group-name	Specifies the AP group name to the DHCP option 82 payload.
flex-group-name	Specifies the FlexConnect group name to the DHCP option 82 payload.
ap-location	Specifies the AP location to the DHCP option 82 payload.
apmac-vlan-id	Specifies the radio MAC address of the access point and the VLAN ID to the DHCP option 82 payload.
apname-vlan-id	Specifies the AP name and its VLAN ID to the DHCP option 82 payload.
ap-ethmac-ssid	Specifies the Ethernet MAC address of the access point and the SSID to the DHCP option 82 payload.

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 remote ID of DHCP option 82 payload:

```
(Cisco Controller) > config dhcp opt-82 remote-id apgroup1
```

config exclusionlist

To create or delete an exclusion list entry, use the **config exclusionlist** command.

config exclusionlist {**add** *MAC* [*description*] | **delete** *MAC* | **description** *MAC* [*description*]}

Syntax Description

config exclusionlist	Configures the exclusion list.
add	Creates a local exclusion-list entry.
delete	Deletes a local exclusion-list entry
description	Specifies the description for an exclusion-list entry.
MAC	MAC address of the local Excluded entry.
description	(Optional) Description, up to 32 characters, for an excluded entry.

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 local exclusion list entry for the MAC address *xx:xx:xx:xx:xx:xx:*

```
(Cisco Controller) > config exclusionlist add xx:xx:xx:xx:xx:xx lab
```

The following example shows how to delete a local exclusion list entry for the MAC address *xx:xx:xx:xx:xx:xx:*

```
(Cisco Controller) > config exclusionlist delete xx:xx:xx:xx:xx:xx lab
```

Related Commands

show exclusionlist

config ldap

To configure the Lightweight Directory Access Protocol (LDAP) server settings, use the **config ldap** command.

config ldap {**add** | **delete** | **enable** | **disable** | **retransmit-timeout** | **retry** | **user** | **simple-bind**} *index*

config ldap add *index server_ip_address port user_base user_attr user_type* [ ]

config ldap retransmit-timeout *index retransmit-timeout*

config ldap retry *attempts*

config ldap user {**attr** *index user-attr* | **base** *index user-base* | **type***index user-type*}

config ldap simple-bind {**anonymous** *index* | **authenticated** *index username password*}

Syntax Description

add	Specifies that an LDAP server is being added.
delete	Specifies that an LDAP server is being deleted.
enable	Specifies that an LDAP serve is enabled.
disable	Specifies that an LDAP server is disabled.
retransmit-timeout	Changes the default retransmit timeout for an LDAP server.
retry	Configures the retry attempts for an LDAP server.
user	Configures the user search parameters.
simple-bind	Configures the local authentication bind method.
anonymous	Allows anonymous access to the LDAP server.
authenticated	Specifies that a username and password be entered to secure access to the LDAP server.
index	LDAP server index. The range is from 1 to 17.
server_ip_address	IP address of the LDAP server.
port	Port number.
user_base	Distinguished name for the subtree that contains all of the users.
user_attr	Attribute that contains the username.
user_type	ObjectType that identifies the user.

retransmit-timeout	Retransmit timeout for an LDAP server. The range is from 2 to 30.
attempts	Number of attempts that each LDAP server is retried.
attr	Configures the attribute that contains the username.
base	Configures the distinguished name of the subtree that contains all the users.
type	Configures the user type.
username	Username for the authenticated bind method.
password	Password for the authenticated bind method.

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 LDAP server index 10:

```
(Cisco Controller) > config ldap enable 10
```

Related Commands

config ldap add

config ldap simple-bind

show ldap summary

config local-auth active-timeout

To specify the amount of time in which the controller attempts to authenticate wireless clients using local Extensible Authentication Protocol (EAP) after any pair of configured RADIUS servers fails, use the **config local-auth active-timeout** command.

config local-auth active-timeout *timeout*

Syntax Description

timeout	Timeout measured in seconds. The range is from 1 to 3600.

Command Default

The default timeout value is 100 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 the active timeout to authenticate wireless clients using EAP to 500 seconds:

```
(Cisco Controller) > config local-auth active-timeout 500
```

Related Commands

clear stats local-auth

config local-auth eap-profile

config local-auth method fast

config local-auth user-credentials

debug aaa local-auth

show local-auth certificates

show local-auth config

show local-auth statistics

config local-auth eap-profile

To configure local Extensible Authentication Protocol (EAP) authentication profiles, use the **config local-auth eap-profile** command.

config local-auth eap-profile {[**add** | **delete**] *profile_name* | **cert-issuer** {**cisco** | **vendor**} | **method** *method* **local-cert** {**enable** | **disable**} *profile_name* | **method** *method* **client-cert** {**enable** | **disable**} *profile_name* | **method** *method* **peer-verify ca-issuer** {**enable** | **disable**} | **method** *method* **peer-verify cn-verify** {**enable** | **disable**} | **method** *method* **peer-verify date-valid** {**enable** | **disable**}

Syntax Description

add	(Optional) Specifies that an EAP profile or method is being added.
delete	(Optional) Specifies that an EAP profile or method is being deleted.
profile_name	EAP profile name (up to 63 alphanumeric characters). Do not include spaces within a profile name.
cert-issuer	(For use with EAP-TLS, PEAP, or EAP-FAST with certificates) Specifies the issuer of the certificates that will be sent to the client. The supported certificate issuers are Cisco or a third-party vendor.
cisco	Specifies the Cisco certificate issuer.
vendor	Specifies the third-party vendor.
method	Configures an EAP profile method.
method	EAP profile method name. The supported methods are leap, fast, tls, and peap.
local-cert	(For use with EAP-FAST) Specifies whether the device certificate on the controller is required for authentication.
enable	Specifies that the parameter is enabled.
disable	Specifies that the parameter is disabled.
client-cert	(For use with EAP-FAST) Specifies whether wireless clients are required to send their device certificates to the controller in order to authenticate.
peer-verify	Configures the peer certificate verification options.
ca-issuer	(For use with EAP-TLS or EAP-FAST with certificates) Specifies whether the incoming certificate from the client is to be validated against the Certificate Authority (CA) certificates on the controller.

cn-verify	(For use with EAP-TLS or EAP-FAST with certificates) Specifies whether the common name (CN) in the incoming certificate is to be validated against the CA certificates' CN on the controller.
date-valid	(For use with EAP-TLS or EAP-FAST with certificates) Specifies whether the controller is to verify that the incoming device certificate is still valid and has not expired.

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 local EAP profile named FAST01:

```
(Cisco Controller) > config local-auth eap-profile add FAST01
```

The following example shows how to add the EAP-FAST method to a local EAP profile:

```
(Cisco Controller) > config local-auth eap-profile method add fast FAST01
```

The following example shows how to specify Cisco as the issuer of the certificates that will be sent to the client for an EAP-FAST profile:

```
(Cisco Controller) > config local-auth eap-profile method fast cert-issuer cisco
```

The following example shows how to specify that the incoming certificate from the client be validated against the CA certificates on the controller:

```
(Cisco Controller) > config local-auth eap-profile method fast peer-verify ca-issuer enable
```

Related Commands

config local-auth active-timeout

config local-auth method fast

config local-auth user-credentials

debug aaa local-auth

show local-auth certificates

show local-auth config

show local-auth statistics

config local-auth method fast

To configure an EAP-FAST profile, use the **config local-auth method fast** command.

config local-auth method fast {**anon-prov** [**enable** | **disable**] | **authority-id** *auth_id* **pac-ttl** *days* | **server-key** *key_value*}

Syntax Description

anon-prov	Configures the controller to allow anonymous provisioning, which allows PACs to be sent automatically to clients that do not have one during Protected Access Credentials (PAC) provisioning.
enable	(Optional) Specifies that the parameter is enabled.
disable	(Optional) Specifies that the parameter is disabled.
authority-id	Configures the authority identifier of the local EAP-FAST server.
auth_id	Authority identifier of the local EAP-FAST server (2 to 32 hexadecimal digits).
pac-ttl	Configures the number of days for the Protected Access Credentials (PAC) to remain viable (also known as the time-to-live [TTL] value).
days	Time-to-live value (TTL) value (1 to 1000 days).
server-key	Configures the server key to encrypt or decrypt PACs.
key_value	Encryption key value (2 to 32 hexadecimal digits).

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 controller to allows anonymous provisioning:

```
(Cisco Controller) > config local-auth method fast anon-prov disable
```

The following example shows how to configure the authority identifier 0125631177 of the local EAP-FAST server:

```
(Cisco Controller) > config local-auth method fast authority-id 0125631177
```

The following example shows how to configure the number of days to 10 for the PAC to remain viable:

```
(Cisco Controller) > config local-auth method fast pac-ttl 10
```

Related Commands

clear stats local-auth

config local-auth eap-profile

config local-auth active-timeout

config local-auth user-credentials

debug aaa local-auth

show local-auth certificates

show local-auth config

show local-auth statistics

config local-auth user-credentials

To configure the local Extensible Authentication Protocol (EAP) authentication database search order for user credentials, use the **config local-auth user credentials** command.

config local-auth user-credentials {**local** [**ldap**] | **ldap** [**local**] }

Syntax Description

local	Specifies that the local database is searched for the user credentials.
ldap	(Optional) Specifies that the Lightweight Directory Access Protocol (LDAP) database is searched for the user credentials.

Command Default

None

Command History

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

Usage Guidelines

The order of the specified database parameters indicate the database search order.

The following example shows how to specify the order in which the local EAP authentication database is searched:

```
(Cisco Controller) > config local-auth user credentials local lda
```

In the above example, the local database is searched first and then the LDAP database.

Related Commands

clear stats local-auth

config local-auth eap-profile

config local-auth method fast

config local-auth active-timeout

debug aaa local-auth

show local-auth certificates

show local-auth config

show local-auth statistics

config ipv6 acl

To create or delete an IPv6 ACL on the Cisco wireless LAN controller, apply ACL to data path, and configure rules in the IPv6 ACL, use the **config ipv6 acl** command.

config ipv6 acl [**apply** | **cpu** | **create** | **delete** | **rule**]
config ipv6 acl apply *name*
config ipv6 acl cpu {*name* | **none**}
config ipv6 acl create *name*
config ipv6 acl delete *name*
config ipv6 acl rule [**action** | **add** | **change** | **delete** | **destination** | **direction** | **dscp** | **protocol** | **source** | **swap**]
config ipv6 acl rule action *name index* {**permit** | **deny**}
config ipv6 acl rule add *name index*
config ipv6 acl rule change index *name old_index new_index*
config ipv6 acl rule delete *name index*
config ipv6 acl rule destination {**address** *name index ip_address prefix-len* | **port range** *name index* }
`config ipv6 acl rule direction` *name index* `{in | out | any}`
config ipv6 acl rule dscp *name dscp*
config ipv6 acl rule protocol *name index protocol*
config ipv6 acl rule source {**address** *name index ip_address prefix-len* | **port range** *name index start_port end_port*}
config ipv6 acl rule swap index *name index_1index_2*

Syntax Description

apply *name*	Applies an IPv6 ACL. An IPv6 ACL can contain up to 32 alphanumeric characters.
cpu *name*	Applies the IPv6 ACL to the CPU.
cpu none	Configure none if you wish not to have a IPV6 ACL.
create	Creates an IPv6 ACL.
delete	Deletes an IPv6 ACL.
rule (**action**) (*name*) (*index*)	Configures rules in the IPv6 ACL to either permit or deny access. IPv6 ACL name can contains up to 32 alphanumeric characters and IPv6 ACL rule index can be between 1 and 32.
{**permit** | **deny**}	Permit or deny the IPv6 rule action.
add *name index*	Adds a new rule and rule index.
change *name old_index new_index*	Changes a rule's index.
delete *name index*	Deletes a rule and rule index.
destination address *name index ip_addr prefix-len*	Configures a rule's destination IP address and prefix length (between 0 and 128).

destination port *name index*	Configure a rule's destination port range. Enter IPv6 ACL name and set an rule index for it.
direction *name index* {**in** | **out** | **any**}	Configures a rule's direction to in, out, or any.
dscp *name index dscp*	Configures a rule's DSCP. For rule index of DSCP, select a number between 0 and 63, or **any**.
protocol *name index protocol*	Configures a rule's protocol. Enter a name and set an index between 0 and 255 or **any**
source address *name index ip_address prefix-len*	Configures a rule's source IP address and netmask.
source port range *name index start_port end_port*	Configures a rule's source port range.
swap index *name index_1 index_2*	Swap's two rules' indices.

Command Default

After adding an ACL, the **config ipv6 acl cpu** is by default configured as **enabled**.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6..
8.0	This command was updated by adding **cpu** and **none** keywords and the *ipv6_acl_name* variable.

Usage Guidelines

For a Cisco 2100 Series Wireless LAN Controller, you must configure a preauthentication ACL on the wireless LAN for the external web server. This ACL should then be set as a wireless LAN preauthentication ACL under Web Policy. However, you do not need to configure any preauthentication ACL for Cisco 4400 Series Wireless LAN Controllers.

The following example shows how to configure an IPv6 ACL to permit access:

```
(Cisco Controller) >config ipv6 acl rule action lab1 4 permit
```

The following example shows how to configure an interface ACL:

```
(Cisco Controller) > config ipv6 interface acl management IPv6-Acl
```

Related Commands

show ipv6 acl detailed

show ipv6 acl cpu

config netuser add

To add a guest user on a WLAN or wired guest LAN to the local user database on the controller, use the **config netuser add** command.

config netuser add *username password* {**wlan** *wlan_id* | **guestlan** *guestlan_id*} **userType guest lifetime** *lifetime* **description** *description*

Syntax Description

username	Guest username. The username can be up to 50 alphanumeric characters.
password	User password. The password can be up to 24 alphanumeric characters.
wlan	Specifies the wireless LAN identifier to associate with or zero for any wireless LAN.
wlan_id	Wireless LAN identifier assigned to the user. A zero value associates the user with any wireless LAN.
guestlan	Specifies the guest LAN identifier to associate with or zero for any wireless LAN.
guestlan_id	Guest LAN ID.
userType	Specifies the user type.
guest	Specifies the guest for the guest user.
lifetime	Specifies the lifetime.
lifetime	Lifetime value (60 to 259200 or 0) in seconds for the guest user. **Note** A value of 0 indicates an unlimited lifetime.
description	Short description of user. The description can be up to 32 characters enclosed in double-quotes.

Command Default

None

Command History

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

Usage Guidelines

Local network usernames must be unique because they are stored in the same database.

The following example shows how to add a permanent username Jane to the wireless network for 1 hour:

```
(Cisco Controller) > config netuser add jane able2 1 wlan_id 1 userType permanent
```

The following example shows how to add a guest username George to the wireless network for 1 hour:

```
(Cisco Controller) > config netuser add george able1 guestlan 1 3600
```

Related Commands

show netuser

config netuser delete

config netuser delete

To delete an existing user from the local network, use the **config netuser delete** command.

config netuser delete *username*

Syntax Description

username	Network username. The username can be 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.

Usage Guidelines

Local network usernames must be unique because they are stored in the same database.

The following example shows how to delete an existing username named able1 from the network:

```
(Cisco Controller) > config netuser delete able1
Deleted user able1
```

Related Commands

show netuser

config netuser description

To add a description to an existing net user, use the **config netuser description** command.

config netuser description *username description*

Syntax Description

username	Network username. The username can contain up to 24 alphanumeric characters.
description	(Optional) User description. The description can be up to 32 alphanumeric characters enclosed in double quotes.

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 user description “HQ1 Contact” to an existing network user named able 1:

```
(Cisco Controller) > config netuser description able1 “HQ1 Contact”
```

Related Commands

show netuser

config network bridging-shared-secret

To configure the bridging shared secret, use the **config network bridging-shared-secret** command.

config network bridging-shared-secret *shared_secret*

Syntax Description

shared_secret	Bridging shared secret string. The string can contain up to 10 bytes.

Command Default

The bridging shared secret is enabled by default.

Command History

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

Usage Guidelines

This command creates a secret that encrypts backhaul user data for the mesh access points that connect to the switch.

The zero-touch configuration must be enabled for this command to work.

The following example shows how to configure the bridging shared secret string “shhh1”:

```
(Cisco Controller) > config network bridging-shared-secret shhh1
```

Related Commands

show network summary

config network web-auth captive-bypass

To configure the controller to support bypass of captive portals at the network level, use the **config network web-auth captive-bypass** command.

config network web-auth captive-bypass {**enable** | **disable**}

Syntax Description

enable	Allows the controller to support bypass of captive portals.
disable	Disallows the controller to support bypass of captive portals.

Command Default

None

The following example shows how to configure the controller to support bypass of captive portals:

```
(Cisco Controller) > config network web-auth captive-bypass enable
```

Related Commands

show network summary

config network web-auth cmcc-support

config network web-auth port

To configure an additional port to be redirected for web authentication at the network level, use the **config network web-auth port** command.

config network web-auth port *port*

Syntax Description

port	Port number. The valid range is from 0 to 65535.

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 additional port number 1200 to be redirected for web authentication:

```
(Cisco Controller) > config network web-auth port 1200
```

Related Commands

show network summary

config network web-auth proxy-redirect

To configure proxy redirect support for web authentication clients, use the **config network web-auth proxy-redirect** command.

config network web-auth proxy-redirect {**enable** | **disable**}

Syntax Description

enable	Allows proxy redirect support for web authentication clients.
disable	Disallows proxy redirect support for web authentication clients.

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 proxy redirect support for web authentication clients:

```
(Cisco Controller) > config network web-auth proxy-redirect enable
```

Related Commands

show network summary

config network web-auth secureweb

To configure the secure web (https) authentication for clients, use the **config network web-auth secureweb** command.

config network web-auth secureweb {**enable** | **disable**}

Syntax Description

enable	Allows secure web (https) authentication for clients.
disable	Disallows secure web (https) authentication for clients. Enables http web authentication for clients.

Command Default

The default secure web (https) authentication for clients is enabled.

Command History

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

Usage Guidelines

If you configure the secure web (https) authentication for clients using the **config network web-auth secureweb disable** command, then you must reboot the Cisco WLC to implement the change.

The following example shows how to enable the secure web (https) authentication for clients:

```
(Cisco Controller) > config network web-auth secureweb enable
```

Related Commands

show network summary

config network webmode

To enable or disable the web mode, use the **config network webmode** command.

config network webmode {**enable** | **disable**}

Syntax Description

enable	Enables the web interface.
disable	Disables the web interface.

Command Default

The default value for the web mode is **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 disable the web interface mode:

```
(Cisco Controller) > config network webmode disable
```

Related Commands

show network summary

config network web-auth

To configure the network-level web authentication options, use the **config network web-auth** command.

config network web-auth {**port** *port-number*} | {**proxy-redirect** {**enable** | **disable**}}

Syntax Description

port	Configures additional ports for web authentication redirection.
port-number	Port number (between 0 and 65535).
proxy-redirect	Configures proxy redirect support for web authentication clients.
enable	Enables proxy redirect support for web authentication clients. **Note** Web-auth proxy redirection will be enabled for ports 80, 8080, and 3128, along with user defined port 345.
disable	Disables proxy redirect support for web authentication clients.

Command Default

The default network-level web authentication value is disabled.

Command History

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

Usage Guidelines

You must reset the system for the configuration to take effect.

The following example shows how to enable proxy redirect support for web authentication clients:

```
(Cisco Controller) > config network web-auth proxy-redirect enable
```

Related Commands

show network summary

show run-config

config qos protocol-type

config policy

To configure a native profiling policy on the Cisco Wireless LAN Controller (WLC), use the **config policy** command.

config policy*policy_name* {**action** {**acl** {**enable** | **disable**} *acl_name* | {**average-data-rate** | **average-realtime-rate** | **burst-data-rate** | **burst-realtime-rate** | **qos** | **session-timeout** | **sleeping-client-timeout** | **vlan**} {**enable** | **disable**}}} | **active** {**add hours** *start _time end _time* **days** *day* | **delete days** *day*} | **create** | **delete** | **match** {**device-type** {**add** | **delete**} *device-type* | **eap-type** {**add** | **delete**} {**eap-fast** | **eap-tls** | **leap** | **peap**} | **role** {*role_name* | **none**}}

Syntax Description

policy_name	Name of a profiling policy.
action	Configures an action for the policy.
acl	Configures an ACL for the policy
enable	Enables an action for the policy.
disable	Disables an action for the policy.
acl_name	Name of an ACL.
average-data-rate	Configures the QoS average data rate.
average-realtime-rate	Configures the QoS average real-time rate.
burst-data-rate	Configures the QoS burst data rate.
burst-realtime-rate	Configures the QoS burst real-time rate.
qos	Configures a QoS action for the policy.
session-timeout	Configures a session timeout action for the policy.
sleeping-client-timeout	Configures a sleeping client timeout for the policy.
vlan	Configures a VLAN action for the policy.
active	Configures the active hours and days for the policy.
add	Adds active hours and days.
hours	Configures active hours for the policy.
start _time	Start time for the policy.
end _time	End time for the policy.
days	Configures the day on the policy must work.

day	Day of the week, such as **mon, tue, wed, thu, fri, sat, sun**. You can also specify daily or weekdays for the policy to occur daily or on all weekdays.
delete	Deletes active hours and days.
create	Creates a policy.
match	Configures a match criteria for the policy.
device-type	Configures a device type match.
device-type	Device type on which the policy must be applied. You can configure up to 16 devices types for a policy.
eap-type	Configures the Extensible Authentication Protocol (EAP) type as a match criteria.
eap-fast	Configures the EAP type as EAP Flexible Authentication via Secure Tunneling (FAST).
eap-tls	Configures the EAP type as EAP Transport Layer Security (TLS).
leap	Configures the EAP type as Lightweight EAP (LEAP).
peap	Configures the EAP type as Protected EAP (PEAP).
role	Configures the user type or user group for the user.
role_name	User type or user group of the user, for example, student, employee. You can configure only one role per policy.
none	Configures no user type or user group for the user.

Command Default

There is no native profiling policy on the Cisco WLC.

Command History

Release	Modification
7.5	This command was introduced.

Usage Guidelines

The maximum number of policies that you can configure is 64.

The following example shows how to configure a role for a policy:

```
(Cisco Controller) > config policy student_policy role student
```

Related Topics

config ap flexconnect policy
config wlan policy
debug policy, on page 166

show policy, on page 203

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.

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
```

Related Topics

show radius acct statistics, on page 208

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 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.

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
```

Related Topics

show radius auth statistics, on page 209

config radius auth callStationIdType

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

config radius auth callStationIdType { | **ap-group-name** | **ap-label-address** | **ap-label-address-ssid** | **ap-location** | **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-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.
vlan-id	Configures the Call Station ID type to use the system's VLAN-ID.

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.

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 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 {**3des** | **aes** | **des**} *index*

Syntax Description

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.

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 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-group-name** | **ap-label-address** | **ap-label-address-ssid** | **ap-location** | **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-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.

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.

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
```

Related Topics

show radius summary, on page 210

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
```

Related Topics

config radius acct, on page 61

config radius auth, on page 72
config tacacs dns, on page 139
debug dns, on page 162

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 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
```

Related Topics

config rogue adhoc, on page 98
config rogue auto-contain level, on page 110
config rogue client, on page 114
config rogue detection, on page 117
config rogue rule, on page 125

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
```

Related Topics

config rogue detection min-rssi, on page 119
config rogue detection monitor-ap, on page 120
show rogue rule summary, on page 241
config rogue detection report-interval, on page 122
config rogue detection security-level, on page 123
config rogue detection transient-rogue-interval, on page 124

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
```

Related Topics

config rogue detection min-rssi, on page 119
config rogue detection monitor-ap, on page 120
show rogue rule summary, on page 241
config rogue detection client-threshold, on page 118
config rogue detection security-level, on page 123
config rogue detection transient-rogue-interval, on page 124

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
```

Related Topics

config rogue detection min-rssi, on page 119
config rogue detection monitor-ap, on page 120
show rogue rule summary, on page 241
config rogue detection client-threshold, on page 118
config rogue detection report-interval, on page 122
config rogue detection transient-rogue-interval, on page 124

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
```

Related Topics

config rogue detection min-rssi, on page 119
config rogue detection monitor-ap, on page 120
show rogue rule summary, on page 241
config rogue detection client-threshold, on page 118
config rogue detection report-interval, on page 122
config rogue detection security-level, on page 123

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
```

Related Topics

config rogue adhoc, on page 98
config rogue auto-contain level, on page 110
config rogue client, on page 114
config rogue detection, on page 117
show rogue ignore-list, on page 237
show rogue rule detailed, on page 239
show rogue rule summary, on page 241
config rogue containment, on page 116
config rogue rule condition ap, on page 129

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 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
```

Related Topics

show tacacs acct statistics, on page 242
show tacacs summary, on page 245

config tacacs athr

To configure TACACS+ authorization server settings, use the **config tacacs athr** command.

config tacacs athr {**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** *1-3 seconds*}

Syntax Description

add	Adds a new TACACS+ authorization server (IPv4 or IPv6).
1-3	TACACS+ server index from 1 to 3.
IP addr	TACACS+ authorization server IP address (IPv4 or IPv6).
port	TACACS+ server TCP port.
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 *1-3seconds*	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+ authorization server index 1 with the IPv4 address 10.0.0.0, port number 49, and secret key 12345678 in ASCII:

```
(Cisco Controller) > config tacacs athr add 1 10.0.0.0 49 ascii 12345678
```

The following example shows how to add a new TACACS+ authorization 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 athr add 1 2001:9:6:40::623 49 ascii 12345678
```

The following example shows how to configure the retransmit timeout of 5 seconds for the TACACS+ authorization server:

```
(Cisco Controller) > config tacacs athr server-timeout 1 5
```

Related Topics

show tacacs athr statistics, on page 243
show tacacs summary, on page 245

config tacacs athr mgmt-server-timeout

To configure a default TACACS+ authorization server timeout for management users, use the **config tacacs athr mgmt-server-timeout** command.

config tacacs athr mgmt-server-timeout *index timeout*

Syntax Description

index	TACACS+ authorization 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+ authorization server timeout for management users:

```
(Cisco Controller) > config tacacs athr mgmt-server-timeout 1 10
```

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
```

Related Topics

show tacacs auth statistics, on page 244
show tacacs summary, on page 245

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
```

Related Topics

config tacacs acct, on page 131
config tacacs athr, on page 133
config tacacs auth, on page 136
debug dns, on page 162

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

debug 11w-pmf

To configure the debugging of 802.11w, use the **debug 11w-pmf** command.

debug 11w-pmf {**all** | **events** | **keys**} {**enable** | **disable**}

Syntax Description

all	Configures the debugging of all 802.11w messages.
keys	Configures the debugging of 802.11w keys.
events	Configures the debugging of 802.11w events.
enable	Enables the debugging of 802.1w options.
disable	Disables the debugging of 802.1w options.

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 debugging of 802.11w keys:

```
(Cisco Controller) >debug 11w-pmf keys enable
```

debug aaa

To configure the debugging of AAA settings, use the **debug aaa** command.

debug aaa {[**all** | **avp-xml** | **detail** | **events** | **packet** | **ldap** | **local-auth** | **tacacs**] [**enable** | **disable**]}

Syntax Description

all	(Optional) Configures the debugging of all AAA messages.
avp-xml	(Optional) Configures debug of AAA Avp xml events.
detail	(Optional) Configures the debugging of AAA errors.
events	(Optional) Configures the debugging of AAA events.
packet	(Optional) Configures the debugging of AAA packets.
ldap	(Optional) Configures the debugging of the AAA Lightweight Directory Access Protocol (LDAP) events.
local-auth	(Optional) Configures the debugging of the AAA local Extensible Authentication Protocol (EAP) events.
tacacs	(Optional) Configures the debugging of the AAA TACACS+ events.
enable	(Optional) Enables the debugging.
disable	(Optional) Disables the debugging.

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 debugging of AAA LDAP events:

```
(Cisco Controller) > debug aaa ldap enable
```

Related Commands

debug aaa local-auth eap

show running-config

debug aaa local-auth

To configure the debugging of AAA local authentication on the Cisco WLC, use the **debug aaa local-auth** command.

debug aaa local-auth {**db** | **shim** | **eap** {**framework** | **method**} {**all** | **errors** | **events** | **packets** | **sm**}} {**enable** | **disable**}

Syntax Description

db	Configures the debugging of the AAA local authentication back-end messages and events.
shim	Configures the debugging of the AAA local authentication shim layer events.
eap	Configures the debugging of the AAA local Extensible Authentication Protocol (EAP) authentication.
framework	Configures the debugging of the local EAP framework.
method	Configures the debugging of local EAP methods.
all	Configures the debugging of local EAP messages.
errors	Configures the debugging of local EAP errors.
events	Configures the debugging of local EAP events.
packets	Configures the debugging of local EAP packets.
sm	Configures the debugging of the local EAP state machine.
enable	Starts the debugging.
disable	Stops the debugging.

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 debugging of the AAA local EAP authentication:

```
(Cisco Controller) > debug aaa local-auth eap method all enable
```

Related Commands

clear stats local-auth

config local-auth active-timeout

config local-auth eap-profile

config local-auth method fast

config local-auth user-credentials

show local-auth certificates

show local-auth config

show local-auth statistics

debug bcast

To configure the debugging of broadcast options, use the **debug bcast** command.

debug bcast {**all** | **error** | **message** | **igmp** | **detail**} {**enable** | **disable**}

Syntax Description

all	Configures the debugging of all broadcast logs.
error	Configures the debugging of broadcast errors.
message	Configures the debugging of broadcast messages.
igmp	Configures the debugging of broadcast IGMP messages.
detail	Configures the debugging of broadcast detailed messages.
enable	Enables the broadcast debugging.
disable	Disables the broadcast debugging.

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 debugging of broadcast messages:

```
(Cisco Controller) > debug bcast message enable
```

The following example shows how to disable the debugging of broadcast mesages:

```
(Cisco Controller) > debug bcast message disable
```

Related Commands

debug disable-all

show sysinfo

debug cckm

To configure the debugging of the Cisco Centralized Key Management options, use the **debug cckm**

debug cckm {**client** | **detailed**} {**enable**| **disable**}

Syntax Description

client	Configures debugging of the Cisco Centralized Key Management of clients.
detailed	Configures detailed debugging of Cisco Centralized Key Management.
enable	Enables debugging of Cisco Centralized Key Management.
disable	Disables debugging of Cisco Centralized Key Management.

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 detailed debugging of Cisco Centralized Key Management:

```
(Cisco Controller) > debug cckm detailed enable
```

debug cts sxp

To configure debugging of Cisco TrustSec SXP options, use the **debug cts sxp** command.

debug cts sxp {**all** | **errors** | **events** | **framework** | **message**} {**enable** | **disable**}

Syntax Description

all	Configures debugging of all the CTS SXP options
errors	Configures debugging of the CTS SXP errors
events	Configures debugging of the CTS SXP events
framework	Configures debugging of the CTS SXP framework
message	Configures debugging of the CTS SXP messages
enable	Enables debugging
disable	Disables debugging

Command Default

None

Command History

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

Related Topics

config cts sxp, on page 32

debug dns

To configure debugging of Domain Name System (DNS) options, use the **debug dns** command.

debug dns {**all** | **detail** | **error** | **message**} {**enable** | **disable**}

Syntax Description

all	Configures debugging of all the DNS options.
detail	Configures debugging of the DNS details.
error	Configures debugging of the DNS errors.
message	Configures debugging of the DNS messages.
enable	Enables debugging of the DNS options.
disable	Disables debugging of the DNS options.

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 DNS error debugging:

```
(Cisco Controller) > debug dns error enable
```

Related Topics

config radius dns, on page 94
config tacacs dns, on page 139

debug dot1x

To configure debugging of the 802.1X options, use the **debug dot1x** command.

debug dot1x {**aaa** | **all** | **events** | **packets** | **states**} {**enable** | **disable**}

Syntax Description

aaa	Configures debugging of the 802.1X AAA interactions.
all	Configures debugging of all the 802.1X messages.
events	Configures debugging of the 802.1X events.
packets	Configures debugging of the 802.1X packets.
states	Configures debugging of the 802.1X state transitions.
enable	Enables debugging of the 802.1X options.
disable	Disables debugging of the 802.1X options.

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 802.1X state transitions debugging:

```
(Cisco Controller) > debug dot1x states enable
```

Related Topics

config wlan security 802.1X
config wlan security wpa akm 802.1x

debug dtls

To configure debugging of the Datagram Transport Layer Security (DTLS) options, use the **debug dtls** command.

debug dtls {**all** | **event** | **packet** | **trace**} {**enable** | **disable**}

Syntax Description

all	Configures debugging of all the DTLS messages.
event	Configures debugging of the DTLS events.
packet	Configures debugging of the DTLS packets.
trace	Configures debugging of the DTLS trace messages.
enable	Enables debugging of the DTLS options.
disable	Disables debugging of the DTLS options.

Command Default

None

Command History

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

Usage Guidelines

The debug actions described here are used in conjunction with CAPWAP troubleshooting.

The following example shows how to enable DTLS packet debugging:

```
(Cisco Controller) > debug dtls packet enable
```

Related Topics

show dtls connections

debug nac

To configure the debugging of Network Access Control (NAC), use the **debug nac** command.

debug nac {**events** | **packet**} {**enable** | **disable**}

Syntax Description

events	Configures the debugging of NAC events.
packet	Configures the debugging of NAC packets.
enable	Enables the NAC debugging.
disable	Disables the NAC debugging.

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 debugging of NAC settings:

```
(Cisco Controller) > debug nac events enable
```

Related Commands

show nac statistics

show nac summary

config guest-lan nac

config wlan nac

debug policy

To configure debugging of policy settings, use the **debug policy** command.

debug policy {**errors** | **events**} {**enable** | **disable**}

Syntax Description

errors	Configures debugging of policy errors.
events	Configures debugging of policy events.
enable	Enables debugging of policy events.
disable	Disables debugging of policy events.

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 debugging of policy errors:

```
(Cisco Controller) >  debug policy errors enable
```

Related Topics

config ap flexconnect policy
config wlan policy
config policy, on page 58
show policy, on page 203
show profiling policy summary, on page 205

debug pm

To configure the debugging of the security policy manager module, use the **debug pm** command.

debug pm {**all disable** | {**config** | **hwcrypto** | **ikemsg** | **init** | **list** | **message** | **pki** | **rng** | **rules** | **sa-export** | **sa-import** | **ssh-l2tp** | **ssh-appgw** | **ssh-engine** | **ssh-int** | **ssh-pmgr** | **ssh-ppp** | **ssh-tcp**} {**enable** | **disable**}}

Syntax Description

all disable	Disables all debugging in the policy manager module.
config	Configures the debugging of the policy manager configuration.
hwcrypto	Configures the debugging of hardware offload events.
ikemsg	Configures the debugging of Internet Key Exchange (IKE) messages.
init	Configures the debugging of policy manager initialization events.
list	Configures the debugging of policy manager list mgmt.
message	Configures the debugging of policy manager message queue events.
pki	Configures the debugging of Public Key Infrastructure (PKI) related events.
rng	Configures the debugging of random number generation.
rules	Configures the debugging of Layer 3 policy events.
sa-export	Configures the debugging of SA export (mobility).
sa-import	Configures the debugging of SA import (mobility).
ssh-l2tp	Configures the debugging of policy manager Layer 2 Tunneling Protocol (l2TP) handling.
ssh-appgw	Configures the debugging of application gateways.
ssh-engine	Configures the debugging of the policy manager engine.
ssh-int	Configures the debugging of the policy manager intercepter.
ssh-pmgr	Configures the debugging of the policy manager.

ssh-ppp	Configures the debugging of policy manager Point To Point Protocol (PPP) handling.
ssh-tcp	Configures the debugging of policy manager TCP handling.
enable	Enables the debugging.
disable	Disables the debugging.

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 debugging of PKI-related events:

```
(Cisco Controller) > debug pm pki enable
```

Related Commands

debug disable-all

debug web-auth

To configure debugging of web-authenticated clients, use the **debug web-auth** command.

debug web-auth {**redirect**{ **enable mac** *mac_address* | **disable**} | **webportal-server** {**enable** | **disable**}}

Syntax Description

redirect	Configures debugging of web-authenticated and redirected clients.
enable	Enables the debugging of web-authenticated clients.
mac	Configures the MAC address of the web-authenticated client.
mac_address	MAC address of the web-authenticated client.
disable	Disables the debugging of web-authenticated clients.
webportal-server	Configures the debugging of portal authentication of clients.

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 debugging of a web authenticated and redirected client:

```
(Cisco Controller) > debug web-auth redirect enable mac xx:xx:xx:xx:xx:xx
```

debug wips

To configure debugging of wireless intrusion prevention system (WIPS), use the **debug wips** command.

debug wips {**all** | **error** | **event** | **nmsp** | **packet**} {**enable** | **disable**}

Syntax Description

all	Configures debugging of all WIPS messages.
error	Configures debugging of WIPS errors.
event	Configures debugging of WIPS events.
nmsp	Configures debugging of WIPS Network Mobility Services Protocol (NMSP) events.
packet	Configures debugging of WIPS packets.
enable	Enables debugging of WIPS.
disable	Disables debugging of WIPS.

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 debugging of all WIPS messages:

```
(Cisco Controller) > debug wips all enable
```

Related Commands

debug client

debug dot11 rogue

show wps summary

show wps wips

debug wps sig

To configure the debugging of Wireless Provisioning Service (WPS) signature settings, use the **debug wps sig** command.

debug wps sig {**enable** | **disable**}

Syntax Description

enable	Enables the debugging for WPS settings.
disable	Disables the debugging for WPS settings.

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 debugging of WPS signature settings:

```
(Cisco Controller) > debug wps sig enable
```

Related Commands

debug wps mfp

debug disable-all

debug wps mfp

To configure the debugging of WPS Management Frame Protection (MFP) settings, use the **debug wps mfp** command.

debug wps mfp {**client** | **capwap** | **detail** | **report** | **mm**} {**enable** | **disable**}

Syntax Description

client	Configures the debugging for client MFP messages.
capwap	Configures the debugging for MFP messages between the controller and access points.
detail	Configures the detailed debugging for MFP messages.
report	Configures the debugging for MFP reporting.
mm	Configures the debugging for MFP mobility (inter-Cisco WLC) messages.
enable	Enables the debugging for WPS MFP settings.
disable	Disables the debugging for WPS MFP settings.

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 debugging of WPS MFP settings:

```
(Cisco Controller) > debug wps mfp detail enable
```

Related Commands

debug disable-all

debug wps sig

show 802.11

To display basic 802.11a, 802.11b/g, or 802.11h network settings, use the **show 802.11** command.

show 802.11 {**a** | **b** | **h**}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
h	Specifies the 802.11h network.

Command Default

None.

This example shows to display basic 802.11a network settings:

```
> show 802.11a
802.11a Network.............................. Enabled
11nSupport................................... Enabled
      802.11a Low Band....................... Enabled
      802.11a Mid Band....................... Enabled
      802.11a High Band...................... Enabled
802.11a Operational Rates
    802.11a 6M Rate.......................... Mandatory
    802.11a 9M Rate.......................... Supported
    802.11a 12M Rate......................... Mandatory
    802.11a 18M Rate......................... Supported
    802.11a 24M Rate......................... Mandatory
    802.11a 36M Rate......................... Supported
    802.11a 48M Rate......................... Supported
    802.11a 54M Rate......................... Supported
802.11n MCS Settings:
    MCS 0.................................... Supported
    MCS 1.................................... Supported
    MCS 2.................................... Supported
    MCS 3.................................... Supported
    MCS 4.................................... Supported
    MCS 5.................................... Supported
    MCS 6.................................... Supported
    MCS 7.................................... Supported
    MCS 8.................................... Supported
    MCS 9.................................... Supported
    MCS 10................................... Supported
    MCS 11................................... Supported
    MCS 12................................... Supported
    MCS 13................................... Supported
    MCS 14................................... Supported
    MCS 15................................... Supported
802.11n Status:
    A-MPDU Tx:
        Priority 0........................... Enabled
        Priority 1........................... Disabled
        Priority 2........................... Disabled
        Priority 3........................... Disabled
        Priority 4........................... Disabled
        Priority 5........................... Disabled
        Priority 6........................... Disabled
```

```
        Priority 7.............................. Disabled
Beacon Interval................................. 100
CF Pollable mandatory........................... Disabled
CF Poll Request mandatory....................... Disabled
--More-- or (q)uit
CFP Period...................................... 4
CFP Maximum Duration............................ 60
Default Channel................................. 36
Default Tx Power Level.......................... 0
DTPC Status..................................... Enabled
Fragmentation Threshold......................... 2346
TI Threshold.................................... -50
Legacy Tx Beamforming setting................... Disabled
Traffic Stream Metrics Status................... Enabled
Expedited BW Request Status..................... Disabled
World Mode...................................... Enabled
EDCA profile type............................... default-wmm
Voice MAC optimization status................... Disabled
Call Admission Control (CAC) configuration
Voice AC:
   Voice AC - Admission control (ACM)............ Disabled
   Voice max RF bandwidth........................ 75
   Voice reserved roaming bandwidth.............. 6
   Voice load-based CAC mode..................... Disabled
   Voice tspec inactivity timeout................ Disabled
   Voice Stream-Size............................. 84000
   Voice Max-Streams............................. 2
Video AC:
   Video AC - Admission control (ACM)............ Disabled
   Video max RF bandwidth........................ Infinite
   Video reserved roaming bandwidth.............. 0
```

This example shows how to display basic 802.11h network settings:

```
> show 802.11h
802.11h ..................................... powerconstraint : 0
802.11h ..................................... channelswitch : Disable
802.11h ..................................... channelswitch mode : 0
```

Related Commands

show ap stats

show ap summary

show client summary

show network

show network summary

show port

show wlan

show aaa auth

To display the configuration settings for the AAA authentication server database, use the **show aaa auth** command.

show aaa auth

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 display the configuration settings for the AAA authentication server database:

```
(Cisco Controller) > show aaa auth
Management authentication server order:
    1..................................... local
    2..................................... tacacs
```

Related Commands

config aaa auth

config aaa auth mgmt

show acl

To display the access control lists (ACLs) that are configured on the controller, use the **show acl** command.

show acl {**cpu** | **detailed** *acl_name* | **summary** | **layer2** { **summary** | **detailed** *acl_name* } }

Syntax Description

cpu	Displays the ACLs configured on the Cisco WLC's central processing unit (CPU).
detailed	Displays detailed information about a specific ACL.
acl_name	ACL name. The name can be up to 32 alphanumeric characters.
summary	Displays a summary of all ACLs configured on the controller.
layer2	Displays the Layer 2 ACLs.

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 display the access control lists on the CPU.

```
(Cisco Controller) >show acl cpu

CPU Acl Name.............................
Wireless Traffic.......................... Disabled
Wired Traffic............................. Disabled
Applied to NPU............................ No
```

The following example shows how to display a summary of the access control lists.

```
(Cisco Controller) > show acl summary

ACL Counter Status              Disabled
-----------------------------------------
IPv4 ACL Name                    Applied
------------------------------- -------
acl1                           Yes
acl2                           Yes
acl3                           Yes
-----------------------------------------
IPv6 ACL Name                    Applied
```

```
-------------------------------- -------
acl6                             No
```

The following example shows how to display the detailed information of the access control lists.

```
(Cisco Controller) > show acl detailed acl_name

     Source              Destination        Source Port Dest Port
I Dir IP Address/Netmask IP Address/Netmask Prot   Range    Range     DSCP
 Action Counter
- --- ------------------ ------------------ ---- --------- --------- -----
 ------ -------
1
Any 0.0.0.0/0.0.0.0    0.0.0.0/0.0.0.0    Any  0-65535   0-65535    0    Deny        0
2
In  0.0.0.0/0.0.0.0    200.200.200.0/     6     80-80   0-65535    Any  Permit      0
                             255.255.255.0
DenyCounter :      0
```

Note The Counter field increments each time a packet matches an ACL rule, and the DenyCounter field increments each time a packet does not match any of the rules.

Related Commands

clear acl counters

config acl apply

config acl counter

config acl cpu

config acl create

config acl delete

config interface acl

config acl rule

show advanced eap

To display Extensible Authentication Protocol (EAP) settings, use the **show advanced eap** command.

show advanced eap

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 display the EAP settings:

```
(Cisco Controller) > show advanced eap
EAP-Identity-Request Timeout (seconds)..... 1
EAP-Identity-Request Max Retries.............. 20
EAP Key-Index for Dynamic WEP................. 0
EAP Max-Login Ignore Identity Response..... enable
EAP-Request Timeout (seconds)................. 1
EAP-Request Max Retries....................... 20
EAPOL-Key Timeout (milliseconds).............. 1000
EAPOL-Key Max Retries......................... 2
```

Related Commands

config advanced eap

config advanced timers eap-identity-request-delay

config advanced timers eap-timeout

show database summary

To display the maximum number of entries in the database, use the **show database summary** command.

show database summary

Syntax Description

This command has no arguments or keywords.

Command Default

None

The following is a sample output of the **show database summary** command:

```
(Cisco Controller) > show database summary
Maximum Database Entries..................... 2048
Maximum Database Entries On Next Reboot...... 2048
Database Contents
    MAC Filter Entries..................... 2
    Exclusion List Entries................. 0
    AP Authorization List Entries.......... 1
    Management Users....................... 1
    Local Network Users.................... 1
        Local Users........................ 1
        Guest Users........................ 0
    Total.................................. 5
```

Related Commands

config database size

show exclusionlist

To display a summary of all clients on the manual exclusion list from associating with the controller, use the **show exclusionlist** command.

show exclusionlist

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.

Usage Guidelines

This command displays all manually excluded MAC addresses.

The following example shows how to display the exclusion list:

```
(Cisco Controller) > show exclusionlist
No manually disabled clients.
Dynamically Disabled Clients
----------------------------
  MAC Address             Exclusion Reason        Time Remaining (in secs)
  -----------             ----------------        ------------------------
00:40:96:b4:82:55         802.1X Failure           51
```

Related Commands

config exclusionlist

show ike

To display active Internet Key Exchange (IKE) security associations (SAs), use the **show ike** command.

show ike {**brief** | **detailed**} *IP_or_MAC_address*

Syntax Description

brief	Displays a brief summary of all active IKE SAs.
detailed	Displays a detailed summary of all active IKE SAs.
IP_or_MAC_address	IP or MAC address of active IKE SA.

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 display the active Internet Key Exchange security associations:

```
(Cisco Controller) > show ike brief 209.165.200.254
```

show IPsec

To display active Internet Protocol Security (IPsec) security associations (SAs), use the **show IPsec** command.

show IPsec {**brief** | **detailed**} *IP_or_MAC_address*

Syntax Description

brief	Displays a brief summary of active IPsec SAs.
detailed	Displays a detailed summary of active IPsec SAs.
IP_or_MAC_address	IP address or MAC address of a device.

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 display brief information about the active Internet Protocol Security (IPsec) security associations (SAs):

```
(Cisco Controller) > show IPsec brief 209.165.200.254
```

Related Commands

config radius acct ipsec authentication

config radius acct ipsec disable

config radius acct ipsec enable

config radius acct ipsec encryption

config radius auth IPsec encryption

config radius auth IPsec authentication

config radius auth IPsec disable

config radius auth IPsec encryption

config radius auth IPsec ike

config trapflags IPsec

config wlan security IPsec disable

config wlan security IPsec enable

config wlan security IPsec authentication

config wlan security IPsec encryption

config wlan security IPsec config

config wlan security IPsec ike authentication

config wlan security IPsec ike dh-group

config wlan security IPsec ike lifetime

config wlan security IPsec ike phase1

config wlan security IPsec ike contivity

show ipv6 acl

To display the IPv6 access control lists (ACLs) that are configured on the controller, use the **show ipv6 acl** command.

show ipv6 acl detailed {*acl_name* | **summary**}

Syntax Description

acl_name	IPv6 ACL name. The name can be up to 32 alphanumeric characters.
detailed	Displays detailed information about a specific 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 display the detailed information of the access control lists:

```
(Cisco Controller) >show ipv6 acl detailed acl6
Rule Index..................................... 1
Direction...................................... Any
IPv6 source prefix............................. ::/0
IPv6 destination prefix........................ ::/0
Protocol....................................... Any
Source Port Range.............................. 0-65535
Destination Port Range......................... 0-65535
DSCP........................................... Any
Flow label..................................... 0
Action......................................... Permit
Counter........................................ 0
Deny Counter................................... 0
```

show ipv6 summary

To display the IPv6 configuration settings, use the **show ipv6 summary** command.

show ipv6 summary

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 displays the output of the **show ipv6 summary** command:

```
(Cisco Controller) >show ipv6 summary
Global Config.............................. Enabled
Reachable-lifetime value................... 30
Stale-lifetime value....................... 300
Down-lifetime value........................ 300
RA Throttling.............................. Disabled
RA Throttling allow at-least............... 1
RA Throttling allow at-most................ no-limit
RA Throttling max-through.................. 5
RA Throttling throttle-period.............. 600
RA Throttling interval-option.............. ignore
NS Mulitcast CacheMiss Forwarding.......... Enabled
NA Mulitcast Forwarding.................... Enabled
IPv6 Capwap UDP Lite....................... Enabled
Operating System IPv6 state ............... Enabled
```

show l2tp

To display Layer 2 Tunneling Protocol (L2TP) sessions, use the **show l2tp** command.

show l2tp {**summary** | *ip_address*}

Syntax Description

summary	Displays all L2TP sessions.
ip_address	IP address.

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 display a summary of all L2TP sessions:

```
(Cisco Controller) > show l2tp summary
LAC_IPaddr LTid LSid RTid RSid ATid ASid State
---------- ---- ---- ---- ---- ---- ---- -----
```

show ldap

To display the Lightweight Directory Access Protocol (LDAP) server information for a particular LDAP server, use the **show ldap** command.

show ldap *index*

Syntax Description

index	LDAP server index. Valid values are from 1 to 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 display the detailed LDAP server information:

```
(Cisco Controller) > show ldap 1
Server Index..................................... 1
Address.......................................... 2.3.1.4
Port............................................. 389
Enabled.......................................... Yes
User DN.......................................... name1
User Attribute................................... attr1
User Type........................................ username1
Retransmit Timeout............................... 3 seconds
Bind Method ..................................... Anonymous
```

Related Commands

config ldap

config ldap add

config ldap simple-bind

show ldap statistics

show ldap summary

show ldap statistics

To display all Lightweight Directory Access Protocol (LDAP) server information, use the **show ldap statistics** command.

show ldap statistics

Syntax Description

This command has no arguments or keywords.

Command History

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

The following example shows how to display the LDAP server statistics:

```
(Cisco Controller) > show ldap statistics
Server Index..................................... 1
Server statistics:
  Initialized OK................................. 0
  Initialization failed.......................... 0
  Initialization retries......................... 0
  Closed OK...................................... 0
Request statistics:
  Received....................................... 0
  Sent........................................... 0
  OK............................................. 0
  Success........................................ 0
  Authentication failed.......................... 0
  Server not found............................... 0
  No received attributes......................... 0
  No passed username............................. 0
  Not connected to server........................ 0
  Internal error................................. 0
  Retries........................................ 0
Server Index..................................... 2
...
```

Related Commands

config ldap

config ldap add

config ldap simple-bind

show ldap

show ldap summary

show ldap summary

To display the current Lightweight Directory Access Protocol (LDAP) server status, use the **show ldap summary** command.

show ldap summary

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 display a summary of configured LDAP servers:

```
(Cisco Controller) > show ldap summary
Idx  Server Address   Port  Enabled
---  ---------------  ----  -------
1    2.3.1.4          389   Yes
2    10.10.20.22      389   Yes
```

Related Commands

config ldap

config ldap add

config ldap simple-bind

show ldap statistics

show ldap

show local-auth certificates

To display local authentication certificate information, use the **show local-auth certificates** command:

show local-auth certificates

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 display the authentication certificate information stored locally:

```
(Cisco Controller) > show local-auth certificates
```

Related Commands

clear stats local-auth

config local-auth active-timeout

config local-auth eap-profile

config local-auth method fast

config local-auth user-credentials

debug aaa local-auth

show local-auth config

show local-auth statistics

show local-auth config

To display local authentication configuration information, use the **show local-auth config** command.

show local-auth config

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 display the local authentication configuration information:

```
(Cisco Controller) > show local-auth config
User credentials database search order:
Primary ..................................... Local DB
Configured EAP profiles:
Name ........................................ fast-test
Certificate issuer ..................... default
Enabled methods ........................ fast
Configured on WLANs ................... 2
EAP Method configuration:
EAP-TLS:
Certificate issuer ..................... default
Peer verification options:
 Check against CA certificates ..... Enabled
 Verify certificate CN identity .... Disabled
 Check certificate date validity ... Enabled
EAP-FAST:
TTL for the PAC ........................ 3 600
Initial client message ................. <none>
Local certificate required ............. No
Client certificate required ........... No
Vendor certificate required ........... No
Anonymous provision allowed ........... Yes
Authenticator ID ...................... 7b7fffffff0000000000000000000000
Authority Information .................. Test
EAP Profile..................................... tls-prof
Enabled methods for this profile .......... tls
Active on WLANs ........................... 1 3EAP Method configuration:
EAP-TLS:
Certificate issuer used ............... cisco
Peer verification options:
 Check against CA certificates ..... disabled
```

```
Verify certificate CN identity .... disabled
Check certificate date validity ... disabled
```

Related Commands

clear stats local-auth

config local-auth active-timeout

config local-auth eap-profile

config local-auth method fast

config local-auth user-credentials

debug aaa local-auth

show local-auth certificates

show local-auth statistics

show local-auth statistics

To display local Extensible Authentication Protocol (EAP) authentication statistics, use the **show local-auth statistics** command:

show local-auth statistics

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 display the local authentication certificate statistics:

```
(Cisco Controller) > show local-auth statistics
Local EAP authentication DB statistics:
Requests received ............................... 14
Responses returned .............................. 14
Requests dropped (no EAP AVP) ................... 0
Requests dropped (other reasons) ................ 0
Authentication timeouts ......................... 0
Authentication statistics:
  Method          Success         Fail
  ------------------------------------
  Unknown               0            0
  LEAP                  0            0
  EAP-FAST              2               0
  EAP-TLS               0            0
  PEAP                  0            0
Local EAP credential request statistics:
Requests sent to LDAP DB ........................ 0
Requests sent to File DB ........................ 2
Requests failed (unable to send) ................ 0
Authentication results received:
  Success ....................................... 2
  Fail .......................................... 0
Certificate operations:
Local device certificate load failures .......... 0
Total peer certificates checked ................. 0
Failures:
  CA issuer check ............................... 0
  CN name not equal to identity ................. 0
  Dates not valid or expired .................... 0
```

Related Commands

clear stats local-auth

config local-auth active-timeout

config local-auth eap-profile

config local-auth method fast

config local-auth user-credentials

debug aaa local-auth

show local-auth config

show local-auth certificates

show nac statistics

To display detailed Network Access Control (NAC) information about a Cisco wireless LAN controller, use the **show nac statistics** command.

show nac statistics

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 display detailed statistics of network access control settings:

```
(Cisco Controller) > show nac statistics
Server Index..................................................... 1
Server Address.....................................................
xxx.xxx.xxx.xxx
Number of requests sent.......................................... 0
Number of retransmissions........................................ 0
Number of requests received...................................... 0
Number of malformed requests received............................ 0
Number of bad auth requests received............................. 0
Number of pending requests....................................... 0
Number of timed out requests..................................... 0
Number of misc dropped request received.......................... 0
Number of requests sent.......................................... 0
```

Related Commands

show nac summary

config guest-lan nac

config wlan nac

debug nac

show nac summary

To display NAC summary information for a Cisco wireless LAN controller, use the **show nac summary** command.

show nac summary

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 display a summary information of network access control settings:

```
(Cisco Controller) > show nac summary
NAC ACL Name ..............................................
Index  Server Address                              Port     State
-----  ---------------------------------------  ----     -----
1      xxx.xxx.xxx.xxx                           13336    Enabled
```

Related Commands

show nac statistics

config guest-lan nac

config wlan nac

debug nac

show netuser

To display the configuration of a particular user in the local user database, use the **show netuser** command.

show netuser {**detail** *user_name* | **guest-roles** | **summary**}

Syntax Description

detail	Displays detailed information about the specified network user.
user_name	Network user.
guest_roles	Displays configured roles for guest users.
summary	Displays a summary of all users in the local user database.

Command Default

None

Command History

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

The following is a sample output of the **show netuser summary** command:

```
(Cisco Controller) > show netuser summary
Maximum logins allowed for a given username ........Unlimited
```

The following is a sample output of the **show netuser detail** command:

```
(Cisco Controller) > show netuser detail john10
username..................................... abc
WLAN Id...................................... Any
Lifetime..................................... Permanent
Description.................................. test user
```

Related Commands

config netuser add

config netuser delete

config netuser description

config netuser guest-role apply

config netuser wlan-id

config netuser guest-roles

show netuser guest-roles

To display a list of the current quality of service (QoS) roles and their bandwidth parameters, use the **show netuser guest-roles** command.

show netuser guest-roles

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.

This example shows how to display a QoS role for the guest network user:

```
(Cisco Controller) > show netuser guest-roles
Role Name............................. Contractor
 Average Data Rate.................... 10
 Burst Data Rate...................... 10
 Average Realtime Rate................ 100
 Burst Realtime Rate.................. 100
Role Name............................. Vendor
 Average Data Rate.................... unconfigured
 Burst Data Rate...................... unconfigured
 Average Realtime Rate................ unconfigured
 Burst Realtime Rate.................. unconfigured
```

Related Commands

config netuser add

config netuser delete

config netuser description

config netuser guest-role apply

config netuser wlan-id

show netuser guest-roles

show netuser

show network

To display the current status of 802.3 bridging for all WLANs, use the **show network** command.

show network

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to display the network details:

```
(Cisco Controller) > show network
```

Related Commands

config network

show network summary

show network multicast mgid detail

show network multicast mgid summary

show network summary

To display the network configuration of the Cisco wireless LAN controller, use the **show network summary** command.

show network summary

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to display a summary configuration:

```
(Cisco Controller) >show network summary
RF-Network Name............................. RF
Web Mode.................................... Disable
Secure Web Mode............................. Enable
Secure Web Mode Cipher-Option High.......... Disable
Secure Web Mode Cipher-Option SSLv2......... Disable
Secure Web Mode RC4 Cipher Preference....... Disable
OCSP........................................ Disabled
OCSP responder URL..........................
Secure Shell (ssh).......................... Enable
Telnet...................................... Enable
Ethernet Multicast Mode..................... Disable   Mode: Ucast
Ethernet Broadcast Mode..................... Disable
Ethernet Multicast Forwarding............... Disable
Ethernet Broadcast Forwarding............... Disable
AP Multicast/Broadcast Mode................. Unicast
IGMP snooping............................... Disabled
IGMP timeout................................ 60 seconds
IGMP Query Interval......................... 20 seconds
MLD snooping................................ Disabled
MLD timeout................................. 60 seconds
MLD query interval.......................... 20 seconds
User Idle Timeout........................... 300 seconds
AP Join Priority............................ Disable
ARP Idle Timeout............................ 300 seconds
ARP Unicast Mode............................ Disabled
Cisco AP Default Master..................... Disable
Mgmt Via Wireless Interface................. Disable
Mgmt Via Dynamic Interface.................. Disable
Bridge MAC filter Config.................... Enable
Bridge Security Mode........................ EAP
Over The Air Provisioning of AP's........... Enable
Apple Talk ................................. Disable
Mesh Full Sector DFS........................ Enable
AP Fallback ................................ Disable
Web Auth CMCC Support ...................... Disabled
Web Auth Redirect Ports .................... 80
Web Auth Proxy Redirect  ................... Disable
Web Auth Captive-Bypass   .................. Disable
Web Auth Secure Web  ....................... Enable
Fast SSID Change ........................... Disabled
AP Discovery - NAT IP Only ................. Enabled
IP/MAC Addr Binding Check .................. Enabled
CCX-lite status ............................ Disable
oeap-600 dual-rlan-ports ................... Disable
```

```
oeap-600 local-network ..................... Enable
mDNS snooping............................... Disabled
mDNS Query Interval......................... 15 minutes

Web Color Theme............................. Default
CAPWAP Prefer Mode.......................... IPv4
```

show ntp-keys

To display network time protocol authentication key details, use the **show ntp-keys** command.

show ntp-keys

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.

This example shows how to display NTP authentication key details:

```
(Cisco Controller) > show ntp-keys
Ntp Authentication Key Details...................
      Key Index
     -----------
         1
         3
```

Related Commands

config time ntp

show policy

To display the summary of the configured policies, and the details and statistics of a policy, use the **show policy** command.

show policy {**summary** | *policy-name* [**statistics**]}

Syntax Description

summary	Displays the summary of configured policies.
policy-name	Name of the policy.
statistics	(Optional) Displays the statistics of a policy.

Command Default

None

Command History

Release	Modification
7.5	This command was introduced.

The following is a sample output of the **show policy summary** command:

```
(Cisco Controller) > show policy summary

Number of Policies..... 2

Policy Index Policy Name
------------ ----------------
1            student-FullAccess
2            teacher-FullAccess
```

The following example shows how to display the details of a policy:

```
(Cisco Controller) > show policy student-FullAccess

Policy Index..................................... 1
Match Role....................................... <none>
Match Eap Type................................... EAP-TLS
ACL.............................................. <none>
QOS.............................................. <none>
Average Data Rate................................ 0
Average Real Time Rate........................... 0
Burst Data Rate.................................. 0
Burst Real Time Rate............................. 0
Vlan Id.......................................... 155
Session Timeout.................................. 1800
Sleeping client timeout.......................... 12

Active Hours
------------
Start Time   End Time      Day
----------   --------      ---
```

```
Match Device Types
------------------
Android
```

The following example shows how to display the statistics of a policy:

```
(Cisco Controller) > show policy student-FullAccess statistics

Policy Index..................................... student-FullAccess
Matching Attributes None......................... 619
No Policy Match.................................. 224
Device Type Match................................ 0
EAP Type Match................................... 0
Role Type Match.................................. 0
Client Disconnected.............................. 4
Acl Applied...................................... 0
Vlan changed..................................... 614
Session Timeout Applied.......................... 4
QoS Applied...................................... 0
Avg Data Rate Applied............................ 0
Avg Real Time Rate Applied....................... 0
Burst Data Rate Applied.......................... 0
Burst Real Time Rate Applied..................... 0
Sleeping-Client-Timeout Applied.................. 0
```

Related Topics

config ap flexconnect policy
config wlan policy
config policy, on page 58
debug policy, on page 166
show profiling policy summary, on page 205

show profiling policy summary

To display local device classification of the Cisco Wireless LAN Controller (WLC), use the **show profiling policy summary** command.

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.5	This command was introduced.

The following is a sample output of the **show profiling policy summary** command:

```
(Cisco Controller) > show profiling policy summary

Number of Builtin Classification Profiles: 88
ID   Name                                          Parent Min CM Valid
==== ============================================= ====== ====== =====

   0 Android                                         None     30   Yes

   1 Apple-Device                                    None     10   Yes

   2 Apple-MacBook                                      1     20   Yes

   3 Apple-iPad                                         1     20   Yes

   4 Apple-iPhone                                       1     20   Yes

   5 Apple-iPod                                         1     20   Yes

   6 Aruba-Device                                    None     10   Yes

   7 Avaya-Device                                    None     10   Yes

   8 Avaya-IP-Phone                                     7     20   Yes

   9 BlackBerry                                      None     20   Yes

  10 Brother-Device                                  None     10   Yes

  11 Canon-Device                                    None     10   Yes

  12 Cisco-Device                                    None     10   Yes

  13 Cisco-IP-Phone                                    12     20   Yes

  14 Cisco-IP-Phone-7945G                              13     70   Yes
```

15	Cisco-IP-Phone-7975	13	70	Yes
16	Cisco-IP-Phone-9971	13	70	Yes
17	Cisco-DMP	12	20	Yes
18	Cisco-DMP-4400	17	70	Yes
19	Cisco-DMP-4310	17	70	Yes
20	Cisco-DMP-4305	17	70	Yes
21	DLink-Device	None	10	Yes
22	Enterasys-Device	None	10	Yes
23	HP-Device	None	10	Yes
24	HP-JetDirect-Printer	23	30	Yes
25	Lexmark-Device	None	10	Yes
26	Lexmark-Printer-E260dn	25	30	Yes
27	Microsoft-Device	None	10	Yes
28	Netgear-Device	None	10	Yes
29	NintendoWII	None	10	Yes
30	Nortel-Device	None	10	Yes
31	Nortel-IP-Phone-2000-Series	30	20	Yes
32	SonyPS3	None	10	Yes
33	XBOX360	27	20	Yes
34	Xerox-Device	None	10	Yes
35	Xerox-Printer-Phaser3250	34	30	Yes
36	Aruba-AP	6	20	Yes
37	Cisco-Access-Point	12	10	Yes
38	Cisco-IP-Conference-Station-7935	13	70	Yes
39	Cisco-IP-Conference-Station-7936	13	70	Yes

```
  40 Cisco-IP-Conference-Station-7937                    13     70    Yes
```

Related Topics

config ap flexconnect policy
config wlan policy
config policy, on page 58
debug policy, on page 166
show policy, on page 203

show radius acct statistics

To display the RADIUS accounting server statistics for the Cisco wireless LAN controller, use the **show radius acct statistics** command.

show radius acct statistics

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 display RADIUS accounting server statistics:

```
(Cisco Controller) > show radius acct statistics
Accounting Servers:
Server Index..................................... 1
Server Address................................... 10.1.17.10
Msg Round Trip Time.............................. 0 (1/100 second)
First Requests................................... 0
Retry Requests................................... 0
Accounting Responses............................. 0
Malformed Msgs................................... 0
Bad Authenticator Msgs........................... 0
Pending Requests................................. 0
Timeout Requests................................. 0
Unknowntype Msgs................................. 0
Other Drops...................................... 0
```

Related Commands

config radius acct

config radius acct ipsec authentication

config radius acct ipsec disable

config radius acct network

show radius auth statistics

show radius summary

show radius auth statistics

To display the RADIUS authentication server statistics for the Cisco wireless LAN controller, use the **show radius auth statistics** command.

show radius auth statistics

This command has no arguments or keyword.

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 display RADIUS authentication server statistics:

```
(Cisco Controller) > show radius auth statistics
Authentication Servers:
  Server Index..................................... 1
  Server Address................................... 209.165.200.10
  Msg Round Trip Time.............................. 0 (1/100 second)
  First Requests................................... 0
  Retry Requests................................... 0
  Accept Responses................................. 0
  Reject Responses................................. 0
  Challenge Responses.............................. 0
  Malformed Msgs................................... 0
  Bad Authenticator Msgs........................... 0
  Pending Requests................................. 0
  Timeout Requests................................. 0
  Unknowntype Msgs................................. 0
  Other Drops...................................... 0
```

Related Commands

config radius auth

config radius auth management

config radius auth network

show radius summary

show radius summary

To display the RADIUS authentication and accounting server summary, use the **show radius summary** command.

show radius summary

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 display a RADIUS authentication server summary:

```
(Cisco Controller) > show radius summary
Vendor Id Backward Compatibility..................... Disabled
Credentials Caching.................................. Disabled
Call Station Id Type................................. IP Address
Administrative Authentication via RADIUS......... Enabled
Authentication Servers
Index  Type  Server Address    Port    State     Tout  RFC-3576  IPsec -
 AuthMod
e/Phase1/Group/Lifetime/Auth/Encr
-----  ----  ---------------  ------  --------  ----  --------  --------------
--------------------------------
Accounting Servers
Index  Type  Server Address    Port    State     Tout  RFC-3576  IPsec -
 AuthMod
e/Phase1/Group/Lifetime/Auth/Encr
-----  ----  ---------------  ------  --------  ----  --------  --------------
--------------------------------
```

Related Commands

show radius auth statistics

show radius acct statistics

show rules

To display the active internal firewall rules, use the **show rules** command.

show rules

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 display active internal firewall rules:

```
(Cisco Controller) > show rules
-------------------------------------------------------
Rule ID.............: 3
Ref count...........: 0
Precedence..........: 99999999
Flags...............: 00000001 ( PASS )
Source IP range:
        (Local stack)
Destination IP range:
        (Local stack)
-------------------------------------------------------
Rule ID.............: 25
Ref count...........: 0
Precedence..........: 99999999
Flags...............: 00000001 ( PASS )
Service Info
        Service name........: GDB
        Protocol............: 6
        Source port low.....: 0
        Source port high....: 0
        Dest port low.......: 1000
        Dest port high......: 1000
Source IP range:
IP High.............: 0.0.0.0
        Interface...........: ANY
Destination IP range:
        (Local stack)
-------------------------------------------------------
```

show switchconfig

To display parameters that apply to the Cisco wireless LAN controller, use the **show switchconfig** command.

show switchconfig

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled.

Command History

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

This example shows how to display parameters that apply to the Cisco wireless LAN controller:

```
(Cisco Controller) >> show switchconfig
802.3x Flow Control Mode..................... Disabled
FIPS prerequisite features................... Enabled
Boot Break................................... Enabled
secret obfuscation........................... Enabled
Strong Password Check Features:
         case-check ...........Disabled
         consecutive-check ....Disabled
         default-check .......Disabled
         username-check ......Disabled
```

Related Commands

config switchconfig mode

config switchconfig secret-obfuscation

config switchconfig strong-pwd

config switchconfig flowcontrol

config switchconfig fips-prerequisite

show stats switch

show rogue adhoc custom summary

To display information about custom rogue ad-hoc rogue access points, use the **show rogue adhoc custom summary** command.

show rogue adhoc custom summary

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 display details of custom rogue ad-hoc rogue access points:

```
(Cisco Controller) > show rogue adhoc custom summary
Number of Adhocs.............................0

MAC Address        State               # APs # Clients Last Heard
-----------------  ------------------ -----  ---------
-----------------------
```

Related Commands

show rogue adhoc detailed

show rogue adhoc summary

show rogue adhoc friendly summary

show rogue adhoc malicious summary

show rogue adhoc unclassified summary

config rogue adhoc

show rogue adhoc detailed

To display details of an ad-hoc rogue access point detected by the Cisco wireless LAN controller, use the **show rogue adhoc client detailed** command.

show rogue adhoc detailed *MAC_address*

Syntax Description

MAC_address	Adhoc rogue MAC address.

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 display detailed ad-hoc rogue MAC address information:

```
(Cisco Controller) > show rogue adhoc client detailed 02:61:ce:8e:a8:8c
Adhoc Rogue MAC address..................... 02:61:ce:8e:a8:8c
Adhoc Rogue BSSID........................... 02:61:ce:8e:a8:8c
State....................................... Alert
First Time Adhoc Rogue was Reported.............. Tue Dec 11 20:45:45
2007
Last Time Adhoc Rogue was Reported.............. Tue Dec 11 20:45:45
2007
Reported By
AP 1
MAC Address............................. 00:14:1b:58:4a:e0
Name.................................... AP0014.1ced.2a60
Radio Type.............................. 802.11b
SSID.................................... rf4k3ap
Channel................................. 3
RSSI.................................... -56 dBm
SNR..................................... 15 dB
Encryption.............................. Disabled
ShortPreamble........................... Disabled
WPA Support............................. Disabled
Last reported by this AP.............. Tue Dec 11 20:45:45 2007
```

Related Commands

config rogue adhoc

show rogue ignore-list

show rogue rule summary

show rogue rule detailed

config rogue rule

show rogue adhoc summary

show rogue adhoc friendly summary

To display information about friendly rogue ad-hoc rogue access points, use the **show rogue adhoc friendly summary** command.

show rogue adhoc friendly summary

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 display information about friendly rogue ad-hoc rogue access points:

```
(Cisco Controller) > show rogue adhoc friendly summary

Number of Adhocs.............................0

MAC Address        State               # APs # Clients Last Heard
-----------------  ------------------- ----- ---------
-----------------------
```

Related Commands

show rogue adhoc custom summary

show rogue adhoc detailed

show rogue adhoc summary

show rogue adhoc malicious summary

show rogue adhoc unclassified summary

config rogue adhoc

show rogue adhoc malicious summary

To display information about malicious rogue ad-hoc rogue access points, use the **show rogue adhoc malicious summary** command.

show rogue adhoc malicious summary

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 display details of malicious rogue ad-hoc rogue access points:

```
(Cisco Controller) > show rogue adhoc malicious summary
Number of Adhocs.............................0

MAC Address        State               # APs # Clients Last Heard
-----------------  ------------------ -----  ---------
-----------------------
```

Related Commands

show rogue adhoc custom summary

show rogue adhoc detailed

show rogue adhoc summary

show rogue adhoc friendly summary

show rogue adhoc unclassified summary

config rogue adhoc

show rogue adhoc unclassified summary

To display information about unclassified rogue ad-hoc rogue access points, use the **show rogue adhoc unclassified summary** command.

show rogue adhoc unclassified summary

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 display information about unclassified rogue ad-hoc rogue access points:

```
(Cisco Controller) > show rogue adhoc unclassified summary

Number of Adhocs.............................0

MAC Address        State               # APs # Clients Last Heard
-----------------  ------------------- ----- ---------
-----------------------
```

Related Commands

show rogue adhoc custom summary

show rogue adhoc detailed

show rogue adhoc summary

show rogue adhoc friendly summary

show rogue adhoc malicious summary

config rogue adhoc

show rogue adhoc summary

To display a summary of the ad-hoc rogue access points detected by the Cisco wireless LAN controller, use the **show rogue adhoc summary** command.

show rogue adhoc summary

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 display a summary of all ad-hoc rogues:

```
(Cisco Controller) > show rogue adhoc summary
Detect and report Ad-Hoc Networks..... Enabled
Client MAC Address   Adhoc BSSID    State  # APs       Last Heard
------------------   -----------    -----    ---       -------
xx:xx:xx:xx:xx:xx    super          Alert    1         Sat Aug  9 21:12:50
 2004
xx:xx:xx:xx:xx:xx                    Alert    1          Aug  9 21:12:50
2003
xx:xx:xx:xx:xx:xx                   Alert    1         Sat Aug  9 21:10:50
 2003
```

Related Commands

config rogue adhoc

show rogue ignore-list

show rogue rule summary

show rogue rule detailed

config rogue rule

show rogue adhoc detailed

show rogue ap custom summary

To display information about custom rogue ad-hoc rogue access points, use the **show rogue ap custom summary** command.

show rogue ap custom summary

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 display details of custom rogue ad-hoc rogue access points:

```
(Cisco Controller) > show rogue ap custom summary

Number of APs.............................0

MAC Address        State               # APs # Clients Last Heard
-----------------  ------------------- ----- ---------
-----------------------
```

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 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

show rogue ap clients

To display details of rogue access point clients detected by the Cisco wireless LAN controller, use the **show rogue ap clients** command.

show rogue ap clients *ap_mac_address*

Syntax Description

ap_mac_address	Rogue access point MAC address.

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 display details of rogue access point clients:

```
(Cisco Controller) > show rogue ap clients xx:xx:xx:xx:xx:xx
MAC Address State # APs Last Heard
----------------- ------------------ ----- -------------------------
00:bb:cd:12:ab:ff Alert 1 Fri Nov 30 11:26:23 2007
```

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 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

show rogue ap detailed

To display details of a rogue access point detected by the Cisco wireless LAN controller, use the **show rogue-ap detailed** command.

show rogue ap detailed *ap_mac_address*

Syntax Description

ap_mac_address	Rogue access point MAC address.

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 display detailed information of a rogue access point:

```
(Cisco Controller) > show rogue ap detailed xx:xx:xx:xx:xx:xx
Rogue BSSID..................................... 00:0b:85:63:d1:94
Is Rogue on Wired Network....................... No
Classification.................................. Unclassified
State........................................... Alert
First Time Rogue was Reported................... Fri Nov 30 11:24:56
2007
Last Time Rogue was Reported.................... Fri Nov 30 11:24:56
2007
Reported By
AP 1
MAC Address.............................. 00:12:44:bb:25:d0
Name..................................... flexconnect
Radio Type............................... 802.11g
SSID..................................... edu-eap
Channel.................................. 6
RSSI..................................... -61 dBm
SNR...................................... -1 dB
Encryption............................... Enabled
ShortPreamble............................ Enabled
WPA Support.............................. Disabled
Last reported by this AP.............. Fri Nov 30 11:24:56 2007
```

This example shows how to display detailed information of a rogue access point with a customized classification:

```
(Cisco Controller) > show rogue ap detailed xx:xx:xx:xx:xx:xx
Rogue BSSID..................................... 00:17:0f:34:48:a0
Is Rogue on Wired Network....................... No
Classification.................................. custom
```

```
Severity Score ................................. 1
Class Name.....................................VeryMalicious
Class Change by................................. Rogue Rule
Classified at .................................. -60 dBm
Classified by................................... c4:0a:cb:a1:18:80

State........................................... Contained
State change by................................. Rogue Rule
First Time Rogue was Reported................... Mon Jun  4 10:31:18
2012
Last Time Rogue was Reported.................... Mon Jun  4 10:31:18
2012
Reported By
    AP 1
        MAC Address............................. c4:0a:cb:a1:18:80
        Name.................................... SHIELD-3600-2027
        Radio Type.............................. 802.11g
        SSID.................................... sri
        Channel................................. 11
        RSSI.................................... -87 dBm
        SNR..................................... 4 dB
        Encryption.............................. Enabled
        ShortPreamble........................... Enabled
        WPA Support............................. Enabled
        Last reported by this AP................. Mon Jun  4 10:31:18
2012
```

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 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

show rogue ap summary

To display a summary of the rogue access points detected by the Cisco wireless LAN controller, use the **show rogue-ap summary** command.

show rogue ap summary{**ssid** | **channel**}

Syntax Description

ssid	Displays specific user-configured SSID of the rogue access point.
channel	Displays specific user-configured radio type and channel of the rogue access point.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	The new keywords **SSID** and **channel** are added.

The following example shows how to display a summary of all rogue access points:

```
(Cisco Controller) > show rogue ap summary

Rogue Location Discovery Protocol.................  Disabled
Rogue ap timeout.................................  1200
Rogue on wire Auto-Contain....................... Disabled
Rogue using our SSID Auto-Contain................ Disabled
Valid client on rogue AP Auto-Contain............ Disabled
Rogue AP timeout................................. 1200
Rogue Detection Report Interval.................. 10
Rogue Detection Min Rssi......................... -128
Rogue Detection Transient Interval............... 0
Rogue Detection Client Num Thershold.............. 0
Total Rogues(AP+Ad-hoc) supported................ 2000
Total Rogues classified.......................... 729

MAC Address        Classification     # APs # Clients Last Heard
-----------------  ------------------ ----- --------- ------------------------
xx:xx:xx:xx:xx:xx  friendly           1     0         Thu Aug  4 18:57:11 2005
xx:xx:xx:xx:xx:xx  malicious          1     0         Thu Aug  4 19:00:11 2005
xx:xx:xx:xx:xx:xx  malicious          1     0         Thu Aug  4 18:57:11 2005
xx:xx:xx:xx:xx:xx  malicious          1     0         Thu Aug  4 18:57:11 2005
```

The following example shows how to display a summary of all rogue access points with SSID as extended parameter.

```
(Cisco Controller) > show rogue ap summary ssid

MAC Address        Class              State      SSID  Security
-------------------------------------------------------------------------------------

xx:xx:xx:xx:xx:xx  Unclassified       Alert       xxx   Open
```

```
xx:xx:xx:xx:xx:xx  Unclassified       Alert       xxx   Open
xx:xx:xx:xx:xx:xx  Pending            Pending     xxx   Open
xx:xx:xx:xx:xx:xx  Unclassified       Alert       xxx   WEP/WPA
```

The following example shows how to display a summary of all rogue access points with channel as extended parameter.

```
(Cisco Controller) > show rogue ap summary channel

MAC Address        Class              State  Det RadioType    Channel RSSIlast/Max)
-------------------------------------------------------------------------------------------------------

xx:xx:xx:xx:xx:xx  Unclassified       Alert  802.11g           11    -53 / -48
xx:xx:xx:xx:xx:xx  Unclassified       Alert  802.11g           11    -53 / -48
xx:xx:xx:xx:xx:xx  Unclassified       Alert  802.11a           149    -74 / -69
xx:xx:xx:xx:xx:xx  Unclassified       Alert  802.11a           149    -74 / -69
xx:xx:xx:xx:xx:xx  Unclassified       Alert  802.11a           149    -74 / -69
```

The following example shows how to display a summary of all rogue access points with both SSID and channel as extended parameters.

```
(Cisco Controller) > show rogue ap summary ssid channel

MAC Address        Class        State    SSID                  Security  Det RadioType
Channel  RSSI(last/Max)
-------------------------------------------------------------------------------------------------------
xx:xx:xx:xx:xx:xx  Unclassified  Alert   dd                    WEP/WPA     802.11n5G
56    -73 / -62
xx:xx:xx:xx:xx:xx  Unclassified  Alert   SSID IS HIDDEN        Open        802.11a
149   -68 / -66
xx:xx:xx:xx:xx:xx  Unclassified  Alert   wlan16                WEP/WPA     802.11n5G
149   -71 / -71
xx:xx:xx:xx:xx:xx  Unclassified  Alert   wlan15                WEP/WPA     802.11n5G
149   -71 / -71
xx:xx:xx:xx:xx:xx  Unclassified  Alert   wlan14                WEP/WPA     802.11n5G
149   -71 / -71
xx:xx:xx:xx:xx:xx  Unclassified  Alert   wlan13                WEP/WPA     802.11n5G
149   -71 / -70
xx:xx:xx:xx:xx:xx  Unclassified  Alert   wlan12                WEP/WPA     802.11n5G
149   -71 / -71
```

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 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

show rogue ap friendly summary

To display a list of the friendly rogue access points detected by the controller, use the **show rogue ap friendly summary** command.

show rogue ap friendly summary

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 display a summary of all friendly rogue access points:

```
(Cisco Controller) > show rogue ap friendly summary
Number of APs.................................... 1
MAC Address       State     # APs  # Clients Last Heard
----------------- ------------------ ----- ---------
---------------------------
XX:XX:XX:XX:XX:XX Internal    1   0  Tue Nov 27 13:52:04 2007
```

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 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

show rogue ap malicious summary

To display a list of the malicious rogue access points detected by the controller, use the **show rogue ap malicious summary** command.

show rogue ap malicious summary

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 display a summary of all malicious rogue access points:

```
(Cisco Controller) > show rogue ap malicious summary
Number of APs.................................... 2
MAC Address       State     # APs  # Clients Last Heard
----------------- ------------------ ----- ---------
---------------------------
XX:XX:XX:XX:XX:XX Alert           1   0  Tue Nov 27 13:52:04 2007
XX:XX:XX:XX:XX:XX Alert           1   0  Tue Nov 27 13:52:04 2007
```

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 unclassified summary

show rogue client detailed

show rogue client summary

show rogue ignore-list

show rogue rule detailed

show rogue rule summary

show rogue ap unclassified summary

To display a list of the unclassified rogue access points detected by the controller, use the **show rogue ap unclassified summary** command.

show rogue ap unclassified summary

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 display a list of all unclassified rogue access points:

```
(Cisco Controller) > show rogue ap unclassified summary
Number of APs.................................... 164
MAC Address      State  # APs # Clients Last Heard
---------------- ------------ ----- --------- ---------------
XX:XX:XX:XX:XX:XX Alert   1       0    Fri Nov 30 11:12:52 2007
XX:XX:XX:XX:XX:XX Alert   1       0    Fri Nov 30 11:29:01 2007
XX:XX:XX:XX:XX:XX Alert   1       0    Fri Nov 30 11:26:23 2007
XX:XX:XX:XX:XX:XX Alert   1       0    Fri Nov 30 11:26:23 2007
```

show rogue auto-contain

To display information about rogue auto-containment, use the **show rogue auto-contain** command.

show rogue auto-contain

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 display information about rogue auto-containment:

```
(Cisco Controller) > show rogue auto-contain
Containment Level.............................. 3
monitor_ap_only................................ false
```

Related Commands

config rogue adhoc

config rogue auto-contain level

show rogue client detailed

To display details of a rogue client detected by a Cisco wireless LAN controller, use the **show rogue client detailed** command.

show rogue client detailed *Rogue_AP MAC_address*

Syntax Description

Rogue_AP	Rogue AP address.
MAC_address	Rogue client MAC address.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.1	The *Rogue_AP* parameter to the **show rogue client detailed** command is added.

The following example shows how to display detailed information for a rogue client:

```
(Cisco Controller) > show rogue client detailed xx:xx:xx:xx:xx:xx
Rogue BSSID..................................... 00:0b:85:23:ea:d1
State........................................... Alert
First Time Rogue was Reported................... Mon Dec 3 21:50:36 2007
Last Time Rogue was Reported.................... Mon Dec 3 21:50:36 2007
Rogue Client IP address......................... Not known
Reported By
AP 1
MAC Address............................. 00:15:c7:82:b6:b0
Name.................................... AP0016.47b2.31ea
Radio Type.............................. 802.11a
RSSI.................................... -71 dBm
SNR..................................... 23 dB
Channel................................. 149
Last reported by this AP.............. Mon Dec 3 21:50:36 2007
```

Related Commands

show rogue client summary

show rogue ignore-list

config rogue rule client

config rogue rule

show rogue client summary

To display a summary of the rogue clients detected by the Cisco wireless LAN controller, use the **show rogue client summary** command.

show rogue client summary

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 display a list of all rogue clients:

```
(Cisco Controller) > show rogue client summary
Validate rogue clients against AAA.............. Disabled
Total Rogue Clients supported................... 2500
Total Rogue Clients present..................... 3
MAC Address        State              # APs Last Heard
-----------------  -----------------  ----- ----------------------
xx:xx:xx:xx:xx:xx  Alert              1     Thu Aug  4 19:00:08 2005
xx:xx:xx:xx:xx:xx  Alert              1     Thu Aug  4 19:00:08 2005
xx:xx:xx:xx:xx:xx  Alert              1     Thu Aug  4 19:00:08 2005
xx:xx:xx:xx:xx:xx  Alert              1     Thu Aug  4 19:00:08 2005
xx:xx:xx:xx:xx:xx  Alert              1     Thu Aug  4 19:00:08 2005
xx:xx:xx:xx:xx:xx  Alert              1     Thu Aug  4 19:00:08 2005
xx:xx:xx:xx:xx:xx  Alert              1     Thu Aug  4 19:09:11 2005
xx:xx:xx:xx:xx:xx  Alert              1     Thu Aug  4 19:03:11 2005
xx:xx:xx:xx:xx:xx  Alert              1     Thu Aug  4 19:03:11 2005
xx:xx:xx:xx:xx:xx  Alert              1     Thu Aug  4 19:09:11 2005
xx:xx:xx:xx:xx:xx  Alert              1     Thu Aug  4 18:57:08 2005
xx:xx:xx:xx:xx:xx  Alert              1     Thu Aug  4 19:12:08 2005
```

Related Commands

show rogue client detailed

show rogue ignore-list

config rogue client

config rogue rule

show rogue ignore-list

To display a list of rogue access points that are configured to be ignored, use the **show rogue ignore-list** command.

show rogue ignore-list

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 display a list of all rogue access points that are configured to be ignored.

```
(Cisco Controller) > show rogue ignore-list

MAC Address
-----------------
xx:xx:xx:xx:xx:xx
```

Related Commands

config rogue adhoc

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

config rogue rule

config trapflags rogueap

show rogue client detailed

show rogue ignore-list

show rogue rule summary

show rogue client summary

show rogue ap unclassified summary

show rogue ap malicious summary

show rogue ap friendly summary

config rogue client

show rogue ap summary

show rogue ap clients

show rogue ap detailed

config rogue rule

show rogue rule detailed

To display detailed information for a specific rogue classification rule, use the **show rogue rule detailed** command.

show rogue rule detailed *rule_name*

Syntax Description

rule_name	Rogue rule 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 display detailed information on a specific rogue classification rule:

```
(Cisco Controller) > show rogue rule detailed Rule2
Priority..................................... 2
Rule Name.................................... Rule2
State........................................ Enabled
Type......................................... Malicious
Severity Score............................... 1
Class Name................................... Very_Malicious
Notify....................................... All
State ....................................... Contain
Match Operation.............................. Any
Hit Count.................................... 352
Total Conditions............................. 2
Condition 1
    type..................................... Client-count
    value.................................... 10
Condition 2
    type..................................... Duration
    value (seconds).......................... 2000
Condition 3
    type..................................... Managed-ssid
    value.................................... Enabled
Condition 4
    type..................................... No-encryption
    value.................................... Enabled
Condition 5
    type..................................... Rssi
    value (dBm).............................. -50
Condition 6
    type..................................... Ssid
    SSID Count............................... 1
    SSID 1................................... test
```

Related Commands

config rogue rule

show rogue ignore-list

show rogue rule summary

show rogue rule summary

To display the rogue classification rules that are configured on the controller, use the **show rogue rule summary** command.

show rogue rule summary

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 display a list of all rogue rules that are configured on the controller:

```
(Cisco Controller) > show rogue rule summary
Priority Rule Name                State    Type          Match Hit Count
-------- ---------------------- -------- ------------- ----- ---------
1        mtest                  Enabled  Malicious     All   0
2        asdfasdf               Enabled  Malicious     All   0
```

The following example shows how to display a list of all rogue rules that are configured on the controller:

```
(Cisco Controller) > show rogue rule summary
Priority         Rule Name                Rule state Class Type   Notify
   State    Match Hit Count
-------- ------------------------------ ----------- ----------- --------
 -------- ------ ---------
1        rule2                          Enabled    Friendly     Global
   Alert    All    234
2        rule1                          Enabled    Custom       Global
   Alert    All    0
```

Related Commands

config rogue rule

show rogue ignore-list

show rogue rule detailed

show tacacs acct statistics

To display detailed radio frequency identification (RFID) information for a specified tag, use the **show tacacs acct statistics** command.

show tacacs acct statistics

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 display detailed RFID information:

```
(Cisco Controller) > show tacacs acct statistics
Accounting Servers:
Server Index..................................... 1
Server Address................................... 10.0.0.0
Msg Round Trip Time.............................. 0 (1/100 second)
First Requests................................... 1
Retry Requests................................... 0
Accounting Response.............................. 0
Accounting Request Success....................... 0
Accounting Request Failure....................... 0
Malformed Msgs................................... 0
Bad Authenticator Msgs........................... 0
Pending Requests................................. -1
Timeout Requests................................. 1
Unknowntype Msgs................................. 0
Other Drops...................................... 0
```

show tacacs athr statistics

To display TACACS+ server authorization statistics, use the **show tacacs athr statistics** command.

show tacacs athr statistics

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 display TACACS server authorization statistics:

```
(Cisco Controller) > show tacacs athr statistics
Authorization Servers:
Server Index..................................... 3
Server Address................................... 10.0.0.3
Msg Round Trip Time.............................. 0 (1/100 second)
First Requests................................... 0
Retry Requests................................... 0
Received Responses............................... 0
Authorization Success............................ 0
Authorization Failure............................ 0
Challenge Responses.............................. 0
Malformed Msgs................................... 0
Bad Authenticator Msgs........................... 0
Pending Requests................................. 0
Timeout Requests................................. 0
Unknowntype Msgs................................. 0
Other Drops...................................... 0
```

Related Commands

config tacacs acct

config tacacs athr

config tacacs auth

show tacacs auth statistics

show tacacs summary

show tacacs auth statistics

To display TACACS+ server authentication statistics, use the **show tacacs auth statistics** command.

show tacacs auth statistics

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 display TACACS server authentication statistics:

```
(Cisco Controller) > show tacacs auth statistics
Authentication Servers:
Server Index..................................... 2
Server Address................................... 10.0.0.2
Msg Round Trip Time.............................. 0 (msec)
First Requests................................... 0
Retry Requests................................... 0
Accept Responses................................. 0
Reject Responses................................. 0
Error Responses.................................. 0
Restart Responses................................ 0
Follow Responses................................. 0
GetData Responses................................ 0
Encrypt no secret Responses...................... 0
Challenge Responses.............................. 0
Malformed Msgs................................... 0
Bad Authenticator Msgs........................... 0
Pending Requests................................. 0
Timeout Requests................................. 0
Unknowntype Msgs................................. 0
Other Drops...................................... 0
```

show tacacs summary

To display TACACS+ server summary information, use the **show tacacs summary** command.

show tacacs summary

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 display TACACS server summary information:

```
(Cisco Controller) > show tacacs summary
Authentication Servers
Idx  Server Address    Port    State     Tout
---  ---------------  ------  --------  ----
2    10.0.0.1         49       Enabled   30
Accounting Servers
Idx  Server Address    Port    State     Tout
---  ---------------  ------  --------  ----
1    10.0.0.0         49      Enabled    5
Authorization Servers
Idx  Server Address    Port    State     Tout
---  ---------------  ------  --------  ----
3    10.0.0.3         49       Enabled   5
Idx  Server Address    Port    State     Tout
---  ---------------  ------  --------  ----
4    2001:9:6:40::623  49       Enabled   5
...
```

Related Commands

config tacacs acct

config tacacs athr

config tacacs auth

show tacacs summary

show tacacs athr statistics

show tacacs auth statistics

show wps ap-authentication summary

To display the access point neighbor authentication configuration on the controller, use the **show wps ap-authentication summary** command.

show wps ap-authentication summary

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 display a summary of the Wireless Protection System (WPS) access point neighbor authentication:

```
(Cisco Controller) > show wps ap-authentication summary
AP neighbor authentication is <disabled>.
Authentication alarm threshold is 1.
RF-Network Name: <B1>
```

Related Commands

config wps ap-authentication

show wps cids-sensor

To display Intrusion Detection System (IDS) sensor summary information or detailed information on a specified Wireless Protection System (WPS) IDS sensor, use the **show wps cids-sensor** command.

show wps cids-sensor {**summary** | **detail** *index*}

Syntax Description

summary	Displays a summary of sensor settings.
detail	Displays all settings for the selected sensor.
index	IDS sensor identifier.

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 display all settings for the selected sensor:

```
(Cisco Controller) > show wps cids-sensor detail1
IP Address..................................... 10.0.0.51
Port........................................... 443
Query Interval................................. 60
Username....................................... Sensor_user1
Cert Fingerprint............................... SHA1:
00:00:00:00:00:00:00:00:
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
Query State.................................... Disabled
Last Query Result.............................. Unknown
Number of Queries Sent......................... 0
```

Related Commands

config wps ap-authentication

show wps mfp

To display Management Frame Protection (MFP) information, use the **show wps mfp** command.

show wps mfp {**summary** | **statistics**}

Syntax Description

summary	Displays the MFP configuration and status.
statistics	Displays MFP statistics.

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 display a summary of the MFP configuration and status:

```
(Cisco Controller) > show wps mfp summary
Global Infrastructure MFP state.................. DISABLED (*all infrastructure
settings are overridden)
Controller Time Source Valid..................... False
                                 WLAN       Infra.      Client
WLAN ID  WLAN Name               Status     Protection  Protection
-------  ----------------------  ---------  ----------  ----------
1        homeap                  Disabled   *Enabled    Optional but inactive
 (WPA2 not configured)
2        7921                    Enabled    *Enabled    Optional but inactive
 (WPA2 not configured)
3        open1                   Enabled    *Enabled    Optional but inactive
 (WPA2 not configured)
4        7920                    Enabled    *Enabled    Optional but inactive
 (WPA2 not configured)
                    Infra.             Operational     --Infra. Capability--
AP Name             Validation  Radio  State           Protection  Validation
------------------  ----------  -----  --------------  ----------  ----------
AP1252AG-EW         *Enabled    b/g    Down            Full        Full
                                a      Down            Full        Full
```

The following example shows how to display the MFP statistics:

```
(Cisco Controller) > show wps mfp statistics
BSSID             Radio Validator AP         Last Source Addr  Found  Error Type
     Count      Frame Types
----------------- ----- -------------------- ----------------- ------ ----------
---- ---------- -----------
no errors
```

Related Commands

config wps mfp

show wps shun-list

To display the Intrusion Detection System (IDS) sensor shun list, use the **show wps shun-list** command.

show wps shun-list

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 display the IDS system sensor shun list:

```
(Cisco Controller) > show wps shun-list
```

Related Commands

config wps shun-list re-sync

show wps signature detail

To display installed signatures, use the **show wps signature detail** command.

show wps signature detail *sig-id*

Syntax Description

sig-id	Signature ID of an installed signature.

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 display information on the attacks detected by standard signature 1:

```
(Cisco Controller) > show wps signature detail 1
Signature-ID..................................... 1
Precedence....................................... 1
Signature Name................................... Bcast deauth
Type............................................. standard
FrameType........................................ management
State............................................ enabled
Action........................................... report
Tracking......................................... per Signature and Mac
Signature Frequency.............................. 500 pkts/interval
Signature Mac Frequency.......................... 300 pkts/interval
Interval......................................... 10 sec
Quiet Time....................................... 300 sec
Description...................................... Broadcast Deauthentication Frame
Patterns:
                0(Header):0x0:0x0
                4(Header):0x0:0x0
```

Related Commands

config wps signature

config wps signature frequency

config wps signature mac-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

show wps signature events

To display more information about the attacks detected by a particular standard or custom signature, use the **show wps signature events** command.

show wps signature events {**summary** | {**standard** | **custom**} *precedenceID* {**summary** | **detailed**}

Syntax Description

summary	Displays all tracking signature summary information.
standard	Displays Standard Intrusion Detection System (IDS) signature settings.
custom	Displays custom IDS signature settings.
precedenceID	Signature precedence identification value.
detailed	Displays tracking source MAC address details.

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 display the number of attacks detected by all enabled signatures:

```
(Cisco Controller) > show wps signature events summary
Precedence  Signature Name        Type       # Events
----------  -------------------- --------  --------
1           Bcast deauth         Standard      2
2           NULL probe resp 1    Standard      1
```

This example shows how to display a summary of information on the attacks detected by standard signature 1:

```
(Cisco Controller) > show wps signature events standard 1 summary
Precedence..................................... 1
Signature Name................................. Bcast deauth
Type........................................... Standard
Number of active events........................ 2
Source MAC Addr    Track Method   Frequency # APs Last Heard
-----------------  -------------- --------- ----- ------------------------
00:a0:f8:58:60:dd  Per Signature  50        1     Wed Oct 25 15:03:05
2006
00:a0:f8:58:60:dd  Per Mac        30        1     Wed Oct 25 15:02:53
2006
```

Related Commands

config wps signature frequency

config wps signature mac-frequency

config wps signature interval

config wps signature quiet-time

config wps signature reset

config wps signature

show wps signature summary

show wps summary

show wps signature summary

To see individual summaries of all of the standard and custom signatures installed on the controller, use the **show wps signature summary** command.

show wps signature summary

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 display a summary of all of the standard and custom signatures:

```
(Cisco Controller) > show wps signature summary
Signature-ID..................................... 1
Precedence....................................... 1
Signature Name................................... Bcast deauth
Type............................................. standard
FrameType........................................ management
State............................................ enabled
Action........................................... report
Tracking......................................... per Signature and Mac
Signature Frequency.............................. 50 pkts/interval
Signature Mac Frequency.......................... 30 pkts/interval
Interval......................................... 1 sec
Quiet Time....................................... 300 sec
Description...................................... Broadcast
Deauthentication Frame
Patterns:
                0(Header):0x00c0:0x00ff
                4(Header):0x01:0x01
...
```

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 summary

config wps signature mac-frequency

config wps signature

show wps summary

To display Wireless Protection System (WPS) summary information, use the **show wps summary** command.

show wps summary

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 display WPS summary information:

```
(Cisco Controller) > show wps summary
Auto-Immune
  Auto-Immune..................................... Disabled
Client Exclusion Policy
  Excessive 802.11-association failures.......... Enabled
  Excessive 802.11-authentication failures....... Enabled
  Excessive 802.1x-authentication................ Enabled
  IP-theft....................................... Enabled
  Excessive Web authentication failure........... Enabled
Trusted AP Policy
  Management Frame Protection.................... Disabled
  Mis-configured AP Action....................... Alarm Only
    Enforced encryption policy................... none
    Enforced preamble policy..................... none
    Enforced radio type policy................... none
    Validate SSID................................ Disabled
  Alert if Trusted AP is missing................. Disabled
  Trusted AP timeout............................. 120
Untrusted AP Policy
  Rogue Location Discovery Protocol.............. Disabled
    RLDP Action.................................. Alarm Only
  Rogue APs
    Rogues AP advertising my SSID................ Alarm Only
    Detect and report Ad-Hoc Networks............ Enabled
  Rogue Clients
    Validate rogue clients against AAA........... Enabled
    Detect trusted clients on rogue APs.......... Alarm Only
  Rogue AP timeout............................... 1300
Signature Policy
  Signature Processing........................... Enabled
...
```

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 mac-frequency

show wps summary

config wps signature

config wps signature interval

show wps wips statistics

To display the current state of the Cisco Wireless Intrusion Prevention System (wIPS) operation on the controller, use the **show wps wips statistics** command.

show wps wips statistics

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 display the statistics of the wIPS operation:

```
(Cisco Controller) > show wps wips statistics
Policy Assignment Requests..... 1
Policy Assignment Responses..... 1
Policy Update Requests..... 0
Policy Update Responses..... 0
Policy Delete Requests..... 0
Policy Delete Responses..... 0
Alarm Updates..... 13572
Device Updates..... 8376
Device Update Requests..... 0
Device Update Responses..... 0
Forensic Updates..... 1001
Invalid WIPS Payloads..... 0
Invalid Messages Received..... 0
NMSP Transmitted Packets..... 22950
NMSP Transmit Packets Dropped..... 0
NMSP Largest Packet..... 1377
```

Related Commands

config 802.11 enable

config ap mode

config ap monitor-mode

show ap config

show ap monitor-mode summary

show wps wips summary

show wps wips summary

To display the adaptive Cisco Wireless Intrusion Prevention System (wIPS) configuration that the Wireless Control System (WCS) forwards to the controller, use the **show wps wips summary** command.

show wps wips summary

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 display a summary of the wIPS configuration:

```
(Cisco Controller) > show wps wips summary
Policy Name..................................... Default
Policy Version.................................. 3
```

Related Commands

config 802.11 enable

config ap mode

config ap monitor-mode

show ap config

show ap monitor-mode summary

show wps wips statistics